PROTEÇÃO DE DADOS PESSOAIS NOS SERVIÇOS DE SAÚDE DIGITAL

Mariana Martins de Carvalho
Olívia Bandeira
Rodrigo Murtinho
(Organizadores)

EDIÇÕES LIVRES

PROTEÇÃO DE DADOS PESSOAIS NOS SERVIÇOS DE SAÚDE DIGITAL


idec

intervozes

ICICT

FIOCRUZ

PROTEÇÃO DE DADOS PESSOAIS NOS SERVIÇOS DE SAÚDE DIGITAL

Mariana Martins de Carvalho
Olívia Bandeira
Rodrigo Murtinho
(Organizadores)

EDIÇÕES LIVRES

Rio de Janeiro
2025

PROTEÇÃO DE DADOS PESSOAIS  EM SERVIÇOS DE SAÚDE DIGITAL

Realização
Instituto de Comunicação Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz)

Intervozes – Coletivo Brasil de Comunicação Social

Instituto de Defesa de Consumidores (Idec)

Coordenação Geral
Rodrigo Murtinho (Icict/Fiocruz)

Aldo Pontes (Icict/Fiocruz)

Marcelo Fornazin (Ensp/ Fiocruz)

Olívia Bandeira (Intervozes)

Matheus Z. Falcão (Idec)

Diogo Moyses (Idec)

Coordenação Executiva
Mariana Martins de Carvalho

Pesquisadoras/es
Agleildes Arichele Leal de Queirós

Fabiana Dias do Nascimento

Juliana Pacetta Ruiz

Maria Luciano

Natália Helou Fazzioni

Paulo Victor Melo

Conselho de Especialistas
Angelica Baptista Silva – Departamento de Direitos Humanos da Escola Nacional de Saúde Pública Sergio Arouca (DIHS/ ENSP/Fiocruz)

Bethânia Almeida – Centro de Integração de Dados e Conhecimentos para a Saúde (Cidacs/Fiocruz Bahia)

Bárbara Simão – Mestre em Direito e Desenvolvimento pela Fundação Getúlio Vargas (FGV Direito SP)

Fernanda Bruno – Professora Adjunta da Universidade Federal do Rio de Janeiro (UFRJ)

Fernanda Lira – Rede Transfeminista de Cuidados Digitais e Rede de Ciberativistas Negras no Brasil

Giliate C. Coelho Neto – Médico Sanitarista e Mestre em Saúde Coletiva (Unifesp)

Jefferson da Costa Lima – Coordenador técnico da Plataforma de Ciência de Dados Aplicada à Saúde (PCDaS/Icict/Fiocruz)

Jonas Valente – Laboratório de Políticas de Comunicação da Faculdade de Comunicação da UnB e pesquisador do Oxford Internet Institute

Marco Túlio Castro – Centro de Desenvolvimento Tecnológico em Saúde (CDTS/Fiocruz)

Paulo Renâ – Aquatune Lab

Rosana Castro – Professora adjunta do Instituto de Medicina Social da Universidade do Estado do Rio de Janeiro (IMS/Uerj)

Stephan Sperling – Médico Assistente e Tutor do Programa de Residência em Medicina de Família e Comunidade da Faculdade de Medicina da Universidade de São Paulo (USP)

Tarcízio Silva – Senior Tech Policy Fellow pela Fundação Mozilla e doutorando do Programa de Pós-Graduação em Ciências Humanas e Sociais da Universidade Federal do ABC (UFABC)

Esta obra integra o projeto "Proteção de Dados Pessoais em Serviços de Saúde Digital", financiado por Emendas Parlamentares dos Deputados Federais Fernanda Melchiona (PSOL/RS) e Luciano Ducci (PSB/PR) recebidas e executadas pela Fiocruz.

Os textos, seus resultados e conclusões são de responsabilidade dos respectivos autores e não representam necessariamente a posição institucional das organizações que realizaram essa obra.

Editoria Científica do Icict

Coordenação
Maria Elisa da Silveira

Edições Livres

Coordenação Geral
Rodrigo Murtinho

Coordenação Editorial
Mauro Campello

Capa e Projeto Gráfico
Mauro Campello

Editoração Eletrônica
Multimeios | Icict | Fiocruz

Revisão
Maria Cristina Antonio Jeronimo

https://doi.org/10.29397/EdicoesLivres/20250100

Ficha catalográfica elaborada pela Biblioteca de Manguinhos / ICICT / FIOCRUZ – RJ, sob a responsabilidade de Regina Maria de Souza – CRB-7: RJ-007438/O.

P967 Proteção de dados pessoais nos serviços de saúde digital [recurso eletrônico] / Mariana Martins de Carvalho, Olívia Bandeira, Rodrigo Murtinho (Organizadores). – Rio de Janeiro : Edições Livres, 2025.
270 p. : il.

1 PDF.
Modo de acesso: World Wide Web.
Esta obra integra o projeto "Proteção de Dados Pessoais em Serviços de Saúde Digital", financiado por Emendas Parlamentares dos Deputados Federais Fernanda Melchiona (PSOL/RS) e Luciano Ducci (PSB/PR) recebidas e executadas pela Fiocruz.
Bibliografia: Inclui bibliografias.
ISBN 978-65-87663-22-7 (Digital)

1. Saúde Digital. 2. Registros Eletrônicos de Saúde. 3. Segurança Computacional. 4. Privacidade. 5. Gerenciamento de Dados. I. Carvalho, Mariana Martins de. II. Bandeira, Olívia. III. Murtinho, Rodrigo.

CDD 025.04

Intervozes – Coletivo Brasil de Comunicação Social

Conselho Diretor
Alfredo Portugal
Ana Veloso
Gabriel Cabral
Gabriel Rosa
Gyssele Mendes
Iano Flávio
Tâmara Terso

Coordenação Executiva
Ana Cláudia Mielke
Iara Moura
Pedro Ekman
Pedro Vilaça
Ramênia Vieira

O Coletivo Intervozes atua desde 2003 na luta pelo direito à comunicação, desenvolvendo pesquisa, produção de conteúdo, litígio estratégico, advocacy, incidência nos e com os territórios, educação popular, campanhas, entre outras ações, com o objetivo de pressionar centros de poder em prol da promoção da liberdade de expressão e de pensamento, da diversidade e pluralidade na mídia, do respeito aos direitos humanos e à democracia e da promoção e defesa de uma internet e de tecnologias livres, abertas e autônomas.

Instituto de Defesa de Consumidores (Idec)

Direção Executiva
Igor Rodrigues Britto

Equipe de Gestão
Marina Nascimento
Renato Barreto
Carla Yue
Christian Printes
Claudia Focking

Equipe de Dados & Saúde (2025)
Camila Leite
Lucas Andrietta
Marina Fernandes
Marina Paullelli
Lucas Marcon
Yuri Hidd
Fernando Gentil

O Idec é uma organização da sociedade civil sem fins lucrativos, que atua para proteger e ampliar os direitos dos/as consumidores/as, de forma independente de governos, partidos políticos e empresas. Desde 1987, atuamos independentemente de interesses ou recursos partidários e de empresas na representação de consumidores/as de todo o país na luta por relações de consumo mais justas e éticas, especialmente nas áreas de telecomunicações e direitos digitais, serviços financeiros, saúde, alimentação adequada e saudável, mobilidade, energia e consumo sustentável.

Sumário

Apresentação

Organizadores 11

Prefácio

Fernando Aith 17

A dataficação da saúde e o neoliberalismo

Sérgio Amadeu da Silveira 27

Injustiças epistêmicas e opacidade algorítmica: desafios persistentes na coleta e no uso de dados pessoais

Tarcízio Silva 39

A proteção de dados de trabalhadores em plataformas de atendimento médico em saúde digital

Jonas C. L. Valente 58

Entre a busca de "origens" e o "planejamento da saúde": uma aproximação etnográfica dos Testes Genéticos Diretos ao Consumidor (TGDC)

Rosana Castro 85

Recodificando a terapia: um estudo de caso do aplicativo Cíngulo

Fernanda Bruno, Paulo Faltay, Paula Cardoso Pereira, Helena Strecker e Manuela Caputo 105

Marcada para morrer cedo: a história de Lorena e o impacto do uso indevido de dados de saúde na vida das pessoas

Giliate C. Coelho Neto 129

Compartilhamento de dados e saúde suplementar: limites e possibilidades do O*open Hhealth*

Bárbara Simão.....138

"CPF pra desconto?": uma perspectiva dos direitos à saúde, à defesa do consumidor e à proteção de dados em farmácias

Matheus Zuliane Falcão, Marina Fernandes, Camila Leite e Rodrigo Murtinho.....158

Governança de dados sobre a saúde como direito humano: uma proposta global

Angélica Baptista Silva e Vanessa de Lima e Souza.....177

Assimetrias informacionais e necessidades urgentes: reflexões sobre a cultura de proteção de dados pessoais a partir da experiência da saúde digital no Brasil

Mariana Martins, Natália Fazzioni e Olívia Bandeira 202

Riscos e vulnerabilidades à proteção de dados pessoais em um contexto de digitalização dos serviços de saúde

Fabiana Dias.....228

A proteção de dados pessoais em serviços de saúde digital: apontamentos sobre documentos nacionais e padrões internacionais

Juliana Ruiz, Maria Luciano e Paulo Victor Melo.....248

Autores.....263

https://doi.org/10.29397/EdicoesLivres/202501Ap

Apresentação

Receber *e-mails* avisando que o medicamento que você costuma comprar está acabando e que você deve fazer uma nova compra e aproveitar esse ou aquele desconto. Entrar nas redes sociais ou no buscador e receber propagandas de um medicamento ou de serviço relacionado a um tratamento ou a um hábito seu. Dar de cara com seus dados pessoais disponíveis na rede mundial de computadores, depois de bancos de dados do Sistema Único de Saúde (SUS) serem hackeados. Receber telefonemas de instituições em que você nunca se credenciou com a oferta de serviços e mercadorias ou ser induzido a informar seus dados em troca de descontos. Certamente você já vivenciou alguma ou algumas dessas experiências nos últimos anos.

Poderíamos citar várias supostas coincidências que nos levaram a refletir sobre o caminho que os nossos dados pessoais estão percorrendo nesse infinito emaranhado de conexões que são possíveis a partir da captura e, principalmente, dos cruzamentos oferecidos por algoritmos pouco conhecidos e pouco transparentes na sua forma de atuação.

O tratamento de dados pessoais é um tema que vem causando preocupação no mundo. Nos últimos anos, a União Europeia, o Brasil e outros países têm discutido essa questão e construído leis no sentido de proteger os dados pessoais. Foi no bojo dessa discussão que o parlamento brasileiro aprovou a Lei Geral de Proteção de Dados Pessoais (LGPD), criou a Autoridade Nacional de Proteção de Dados (ANPD) e incluiu a proteção de dados pessoais como um direito fundamental na Constituição Federal.

Nessa discussão, os dados de saúde são considerados dados sensíveis e, ao passo que a lei prevê critérios mais rígidos para utilização desse tipo de dados, a realidade mostra que a aplicação da lei para a proteção de nossos dados na prática é cheia de desafios. Nesse sentido, pesquisadores(as) têm se debruçado sobre o tema para apresentar reflexões e contribuir com os rumos desse debate, fazendo alertas e propondo caminhos.

Esta coletânea é uma dessas contribuições e traz uma série de análises que têm como ponto de partida os dados da pesquisa "Proteção de dados pessoais em serviços de saúde digital", realizada pelo Instituto de Comunicação e Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz), pelo Intervozes – Coletivo Brasil de Comunicação Social – e pelo Instituto Brasileiro de

Defesa de Consumidores (Idec). A pesquisa foi realizada entre os anos de 2021 e 2022 e teve o objetivo de contribuir para a compreensão dos processos de digitalização e de tratamento de dados nos serviços de saúde, como também teve o propósito de refletir sobre o papel de uma cultura de proteção de dados pessoais na área da saúde, tendo como referência a LGPD.

Desde o início, buscamos uma abordagem do tema a partir da diversidade e pluralidade de olhares. Para tanto, a equipe foi composta não apenas por pesquisadoras(es) do direito, por onde circula a maior parte das contribuições acadêmicas sobre o assunto, mas também da saúde – tentando contemplar um pouco a heterogeneidade desse campo –, da comunicação, da antropologia e da informática. Outra ambição foi, tanto na composição da equipe de pesquisadoras(es) quanto do conselho de especialistas, buscar representações da diversidade de raça, gênero e de regiões do país, para além da diversidade de olhares já mencionada. Dessa forma, a coletânea buscou seguir a mesma linha e reuniu contribuições de pesquisadores do projeto, de membros do Conselho de Especialistas e convidados.

O objetivo desta publicação foi, portanto, criar um espaço em que fosse possível ampliar ainda mais a reflexão sobre o tema ao reunir trabalhos de pesquisadores que atuaram no projeto em diálogo com especialistas que participaram do nosso conselho, além de outros trabalhos de pesquisadores que se dedicam a esse objeto de estudo. Esse diálogo, que se impôs como imperativo para alargar o olhar inicial, materializou-se em mais uma importante contribuição, qual seja: a compreensão das relações entre proteção de dados pessoais e saúde em um contexto de crescimento vertiginoso da produção de dados pessoais, da dataficação/datificação da vida e da plataformização das relações mercadológicas e sociais –, considerando-se, sobretudo, o uso de tecnologias digitais.

A coletânea tem início com dois textos que apresentam análises teóricas que ajudam a localizar a dataficação, a plataformização, o colonialismo de dados e a colonização da vida, a partir dos dados dentro das estratégias contemporâneas do neoliberalismo. Sérgio Amadeu da Silveira abre esta coletânea com o texto "A dataficação da saúde e o neoliberalismo". Com a propriedade de quem vem debatendo esse tema sobre diversos aspectos, Silveira nos convida a refletir sobre a penetração do pensamento neoliberal na saúde e, mais especificamente, no SUS, a partir da análise dos principais elementos discursivos do neoliberalismo presentes no programa "Estratégia de saúde digital para o Brasil 2020-2028", lançado em 2020 pelo Ministério da Saúde (MS).

Lançando luz sobre os principais desafios da relação entre dados e saúde, o capítulo seguinte é assinado por Tarcízio Silva e trata das "Injustiças epistêmicas e opacidade algorítmica: desafios persistentes na coleta e no uso de dados pessoais". Silva defende que: "A lente da injustiça epistêmica permite entender danos e vantagens individuais ou coletivas resultantes da distribuição de credibilidade de indivíduos ou grupos na produção e enunciação de conhecimento. E, na mesma chave que propõe Sérgio Amadeu da Silveira no artigo que abre esta coletânea, problematiza as formas como a ideologia neoliberal se materializa e se reinventa na dataficação. Em um diálogo com Miranda Fricker (2007), Silva aprofunda as diferentes formas que a Inteligência Artificial (IA) e os algoritmos reproduzem, por exemplo, o machismo, o patriarcado e o colonialismo, e os reflexos que isso pode ter na gestão da saúde. Por fim, o autor propõe "oferecer caminhos para o avanço do debate sobre a adaptação de políticas e compromissos públicos

Em seguida, a coletânea apresenta uma série de textos baseados em estudos de caso de aplicativos privados utilizados na saúde e de políticas públicas da área. No capítulo "A proteção de dados de trabalhadores em plataformas de atendimento médico em saúde digital", Jonas C. L. Valente se propõe a analisar a intersecção entre saúde digital, trabalho em plataformas e proteção de dados, a partir do estudo de caso de três plataformas de telemedicina: Doctoralia, Conexa Saúde e Docway. O capítulo busca aferir os graus de vigilância e níveis de respeito à proteção de dados, articulando os parâmetros de proteção de dados como o respeito aos direitos trabalhistas.

Na sequência, outro importante estudo de caso é assinado pela antropóloga e professora da Uerj Rosana Castro. No texto "Entre a busca de 'origens' e o 'planejamento da saúde': uma aproximação etnográfica dos Testes Genéticos Diretos ao Consumidor (TGDC)", a autora chama atenção para a circulação de dados de saúde, ou seja, de dados sensíveis, por meio dos testes genéticos que se popularizaram no Brasil, justamente nos anos da pandemia. Castro discute os dilemas e as questões relacionadas aos limites e às possibilidades da LGPD de garantir a proteção de dados genéticos nesse contexto altamente dinâmico e competitivo.

Ainda na problematização de serviços de "saúde" e "bem-estar" empacotados pelo mercado de forma a vender respostas e soluções rápidas, práticas e voltadas para o indivíduo, seja por meio de possíveis antecipações de diagnósticos seja pelo autoconhecimento, a equipe do MediaLab/UFRJ, coordenada pela professora Fernanda Bruno, escreve o texto "Recodificando a terapia: um estudo de caso do aplicativo Cíngulo". O artigo é assinado ainda por Paulo Faltay, Paula Cardoso

Pereira, Helena Strecker e Manuela Caputo e é mais uma etapa da pesquisa sobre aplicativos móveis orientados para a saúde mental e o bem-estar psíquico realizada por esse laboratório.

Os dois capítulos seguintes tratam do Open Health, plataforma proposta para unificar os dados dos sistemas público e privado de saúde, permitindo compartilhamento e portabilidade. A partir de um caso fictício e usando como pano de fundo a discussão sobre o Open Health, o pesquisador Giliate C. Coelho Neto, no texto "Marcada para morrer cedo: a história de Lorena e o impacto do uso indevido de dados de saúde na vida das pessoas", consegue materializar parcela importante do debate da proteção de dados trazendo-o para a vida prática. Repercussões que, muitas vezes, o cidadão e a cidadã que não acompanham o tema no seu cotidiano não teriam elementos para compreender a gravidade do mercado de dados sensíveis, são evidenciadas em um diálogo entre amigos. Já a pesquisadora Bárbara Simão no artigo "Compartilhamento de dados e saúde suplementar: limites e possibilidades do Open Health" compara a plataforma com o Open Banking, apontando cuidados fundamentais, que não podem ser perdidos de vista, em situações em que está previsto o compartilhamento de dados sensíveis.

No capítulo "'CPF pra desconto?': uma perspectiva dos direitos à saúde, à defesa do consumidor e à proteção de dados em farmácias", Matheus Zuliane Falcão, Marina Fernandes, Camila Leite e Rodrigo Murtinho analisam a prática de coleta de dados pessoais pelo varejo farmacêutico no contexto da economia digital. Com base em uma abordagem de saúde digital alinhada aos princípios do SUS e aos direitos humanos, o artigo demonstra como a coleta de informações em torno do número do Cadastro de Pessoas Físicas (CPF) contraria essa perspectiva. A argumentação se sustenta na análise da função econômica dos dados em saúde, no mapeamento do mercado e no histórico recente de iniciativas voltadas à defesa dos direitos à saúde, à proteção de dados pessoais e à defesa do consumidor. Os autores evidenciam como essas práticas de coleta de dados, especialmente nas farmácias, têm sido alvo de críticas e enfrentamentos por parte de entidades e movimentos comprometidos com esses direitos.

O texto das professoras Angélica Baptista Silva e de Vanessa de Lima e Souza traz uma tradução adaptada dos princípios de Governança de Dados Sobre a Saúde (GDSAS) que foram conduzidos e desenvolvidos pela sociedade civil, a partir de um processo inclusivo e consultivo, administrado pela Coalizão Transform Health entre 2020 e 2022. A formulação reuniu cerca de 200 colaboradores de mais de 130 organizações, em oito oficinas globais e regionais, e foi seguida de uma consulta pública mundialmente divulgada de princípios. Esse processo foi idealizado para

reunir diferentes perspectivas e conhecimentos, e garantir o envolvimento de diversas partes interessadas de todas as geografias e os setores, inclusive o Brasil.

A coletânea termina com três capítulos que apresentam de forma mais detalhada os dados da nossa pesquisa "Proteção de dados pessoais em serviços de saúde digital". No texto "Assimetrias informacionais e necessidades urgentes: reflexões sobre a cultura de proteção de dados pessoais a partir da experiência da saúde digital no Brasil", Mariana Martins de Carvalho, Natália Fazzioni e Olívia Bandeira, a partir das percepções dos(as) usuários(as) traçadas por meio de dezesseis entrevistas em profundidade realizadas com usuários(as) dos serviços de saúde que vivem com diabetes, observam de que forma eles entendem a proteção de dados pessoais e de que maneira as percepções sobre o assunto são acionadas em suas vivências cotidianas, problematizando, assim, a noção de "cultura de proteção de dados pessoais", que deve ser compreendida não como uma cartilha de práticas a serem seguidas, mas como respostas de políticas públicas diante dos fluxos globais do mercado de dados pessoais no contexto brasileiro.

No capítulo "Riscos *e vulnerabilidades à proteção de dados* pessoais em um contexto de digitalização dos serviços de saúde, Fabiana Dias, com a colaboração de Liu Leal de Queirós (*in memoriam*), identifica e analisa a monetização dos dados, o perfilamento de comportamento, a confidencialidade, a privacidade e a segurança da informação como os aspectos mais abordados nos estudos acadêmicos que focam nas situações de riscos e vulnerabilidades à proteção de dados pessoais na área da saúde. Esse panorama reflete a ausência de uma política nacional de segurança dos dados, o que implica garantia da proteção de dados pessoais como um direito e a necessária adequação dos serviços às normativas legais vigentes de proteção de dados pessoais. A adequação da prática da saúde às normas de proteção de dados é tema também do texto que fecha a coletânea, "A proteção de dados pessoais em serviços de saúde digital: apontamentos sobre documentos nacionais e padrões internacionais", de Juliana Ruiz, Maria Luciano e Paulo Victor Melo. Os autores analisam documentos nacionais de governos, conselhos de saúde e de outros órgãos, assim como documentos internacionais, e indicam a necessidade de superação de uma espécie de "confusão conceitual" sobre privacidade e proteção de dados pessoais; de detalhamento dos mecanismos de segurança dos dados; de inclusão de marcadores étnico-raciais, de gênero, território, entre outros; e de adequação, no caso de normas de conselhos profissionais, a legislações protetivas, a exemplo da LGPD.

Cabe destacar também o prefácio intitulado *"A proteção de dados em face da transformação digital dos sistemas de saúde modernos"*, gentilmente escrito

pelo professor Fernando Aith, diretor-geral do Centro de Pesquisas de Direito Sanitário da USP (Cepedisa/USP). Nele, o autor analisa de forma concisa as mudanças provocadas pela transformação digital na área da saúde, processo que tem delineado o emergente campo da saúde digital. A partir desse panorama, o professor Aith articula as diferentes perspectivas presentes nos capítulos desta obra, ressaltando a importância de uma abordagem multidisciplinar e crítica. Destaca, em particular, que os avanços tecnológicos devem ser avaliados não apenas por seus benefícios operacionais e assistenciais, mas também pelos riscos éticos e jurídicos que podem comprometer direitos fundamentais — sobretudo no que se refere à proteção de dados pessoais sensíveis. Tal reflexão impõe desafios regulatórios cada vez mais complexos, exigindo marcos normativos sólidos e mecanismos eficazes de governança digital em saúde.

Esperamos que esta coletânea seja capaz de contribuir para o debate sobre proteção de dados pessoais nos serviços de saúde digital no Brasil, mas que também ajude a pensar e construir estratégias para a promoção de uma cultura de proteção de dados com base na garantia de direitos da população que leve em consideração a realidade do país e a da população em que essa pesquisa foi realizada e para quem esse esforço acadêmico se dedica.

Dedicamos este livro à memória de Liu Leal de Queirós.

Boa leitura!

Os organizadores

https://doi.org/10.29397/EdicoesLivres/202501Pr

Prefácio

A proteção de dados em face da transformação digital dos sistemas de saúde modernos

O século XXI é o século da consolidação e evolução do mundo digital.

As inovações da vida moderna digital estão revolucionando as sociedades em diversas dimensões, abrangendo também o setor da saúde e impactando direitos e formas de viver em todo o globo. O mundo digital, com suas múltiplas e variadas bases de dados digitais armazenadas, trata e usa informações sensíveis sobre a saúde dos indivíduos. Esse cenário amplia-se com grande velocidade por meio das novas tecnologias que utilizam o aprendizado automatizado de máquina e/ou a Inteligência Artificial (IA).

Na área da saúde, as tecnologias digitais já estão presentes em vários campos, sendo aplicadas para fins diagnósticos e terapêuticos. Ao mesmo tempo, os fluxos de informações se aceleram, em especial por meio de redes sociais digitais globais altamente conectadas e controladas por grandes corporações digitais. Dessa forma, essas redes começam a fazer circular uma quantidade imensurável de dados e informações de saúde, com imensuráveis potenciais econômicos e sociais.

Transformação digital dos sistemas de saúde

Atualmente, no dia a dia dos sistemas de saúde ao redor do mundo, é cada vez mais frequente nos depararmos com um aparato tecnológico sem precedentes: equipamentos médicos de IA com capacidade de realizar cirurgias complexas apenas com a supervisão humana (em alguns casos, até prescindindo do ser humano para o desempenho de tarefas complexas); dispositivos laboratoriais de diagnóstico que se utilizam da nuvem de dados digitais e da IA para laudos diagnósticos conclusivos; bases de dados gigantes, organizadas e de 'propriedade' de grandes grupos corporativos privados, com alto potencial de lucro em sua utilização (monetização das bases de dados digitais); dispositivos médicos capazes de realizar anamnese, diagnóstico e, ainda, fazer uma proposta terapêutica para o paciente; serviços digitais de compra e venda de produtos de saúde, incluindo

drogas de uso restrito e medicamentos; *softwares* de gestão e governança de serviços públicos e privados de saúde, que cada vez mais ocupam papel de protagonismo na organização de filas, fluxos e prioridades de atendimentos; aplicativos de internet que captam dados sensíveis das pessoas e prescrevem dicas ou orientações de comportamentos no campo da saúde física e mental etc.

Esse conjunto abrangente de produtos e serviços de saúde que se utilizam das novas tecnologias digitais vem formando um campo de estudo que, genericamente, está sendo denominado 'saúde digital'. Para além dos benefícios enormes que essas inovações do campo da saúde digital podem trazer, já está evidenciado que esses produtos, se não fiscalizados e desenvolvidos com ética e responsabilidade, podem produzir danos físicos, psicológicos e morais nos seus usuários, inclusive com resultado de morte. Podem, também, ser instrumentos de violação de direitos fundamentais reconhecidos pelas legislações internacional e nacional, tais como os direitos de intimidade, privacidade, segurança, propriedade, saúde, entre outros.

No âmbito da saúde digital, a proteção de dados pessoais e o uso desses dados para o aprendizado das máquinas destacam-se como temas estratégicos a serem compreendidos e regulados. Ferramentas de IA servem para melhorar a qualidade, a segurança e a eficiência dos cuidados de saúde. No entanto, essas ferramentas usam, usarão e serão usadas para rastrear dados de pacientes, selecionar pacientes, fazer triagem, ler imagens médicas, diagnosticar doenças, tomar decisões de tratamento, apoiar pacientes na promoção da saúde e fornecer cuidados primários, agudos, mentais e de longo prazo. Prevê-se que as inovações de IA não apenas ajudem, mas potencialmente substituam os cuidadores humanos, prestadores de serviços médicos, diagnosticadores e tomadores de decisão especializados.

Nesse novo mundo digital, os dados são o 'ouro' do século XXI. A proteção adequada desses dados é fundamental tanto para gerar um ambiente de negócios saudável quanto para proteger os direitos fundamentais do ser humano, além de garantir que tais tecnologias sejam benéficas à sociedade e aos indivíduos.

Compreender os desafios impostos à sociedade nesse momento mostra-se estratégico para que possamos usufruir do melhor dessas inovações, sem, contudo, expor os indivíduos e a sociedade como um todo a riscos individuais e coletivos desnecessários e, até, letais.

Há uma tensão inerente aos sistemas de saúde de todo mundo, que coloca frente à frente os interesses do empreendedorismo privado e o interesse público. Este deve ser protegido por uma adequada regulação estatal, que ainda se mostra precária e

insuficiente não só no Brasil, mas ao redor do globo. Essa tensão entre interesses privados e interesses públicos associados às novas tecnologias começa a ser verificada em maior escala atualmente no campo da saúde digital, especialmente em decorrência dos avanços que esse campo obteve ao longo da pandemia da covid-19. Encaixam-se nesse cenário os atuais debates regulatórios que estão sendo travados na sociedade sobre a coleta, o armazenamento e o uso de dados pessoais para fins de monetização, pesquisas, formulação de políticas públicas e para fins de uso no aprendizado de máquina.

No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD, lei n. 13.709/2018), inspirada no regulamento europeu aprovado alguns anos antes, criou a Autoridade Nacional de Proteção de Dados (ANPD) e representou um importante avanço regulatório com impactos positivos sobre a saúde digital. No entanto, a eficácia do atual modelo regulatório ainda é tímida. É preciso continuar de forma permanente e altamente qualificada o processo de construção e aperfeiçoamento sobre a governança destinada à proteção de dados no país.

Considerando a incipiente legislação vigente no país sobre o tema, aliada cada vez mais à fragilizada organização institucional e de governança estatal para o eficiente exercício do poder regulatório estatal no campo da saúde digital, é fundamental que as sociedades brasileira e global desenvolvam capacidade crítica de compreensão do fenômeno e busquem soluções inovadoras e humanizadas para o uso das tecnologias digitais aplicado ao campo da saúde.

Desafios regulatórios sobre proteção de dados de saúde na era da saúde digital

Um dos grandes desafios do sistema de saúde brasileiro para os próximos anos será o de regular adequadamente a coleta, o armazenamento, o tratamento, o uso, o comércio e a disponibilização dos dados digitais coletados e armazenados por diversas plataformas e aplicativos digitais de saúde que estão em funcionamento e são amplamente difundidos no mercado. Os dados relacionados à saúde de uma pessoa são, via de regra, considerados 'dados sensíveis', na medida em que reúnem informações que, tradicionalmente, encontram-se no campo dos direitos de personalidade.

Dados típicos da personalidade da pessoa, tais como nome, endereço, idade, sexo, estado civil, gênero e cor, entre outros, são associados, nas plataformas e nos aplicativos digitais de saúde, a dados sensíveis e ultrassensíveis relacionados ao

estado de saúde da pessoa, tais como hábitos alimentares, hábitos de exercício físico, condições de saúde, cirurgias já realizadas, medicamentos já usados e em utilização, exames diagnósticos laboratoriais, tratamentos realizados, doenças antigas e atuais etc. A depender do tipo de informação de saúde da pessoa, podemos dizer que são dados ultrassensíveis, que exigem grande proteção estatal, em nível igual ou ainda superior à proteção atualmente dada para os dados fiscais e bancários de um cidadão.

Nos tempos atuais, em que praticamente todas as ações cotidianas da vida estão mediadas por plataformas e aplicativos digitais, a quantidade de dados e informações pessoais de cada um de nós que está na posse de terceiros é enorme, gerando uma nova forma de vulnerabilidade que podemos classificar como 'vulnerabilidade digital'. A vulnerabilidade digital tem como causa não só a dimensão dos dados pessoais expostos a terceiros nas plataformas e nos aplicativos digitais, mas também a fragilidade dos cidadãos nesses tempos de revolução digital no que se refere ao recebimento diuturno de serviços digitais de saúde que podem, no final das contas, mais prejudicar do que beneficiar a saúde das pessoas. São os *sites* e aplicativos que vendem bem-estar, serviços diagnósticos e terapêuticos de saúde, produtos de saúde e medicamentos, enfim, são eles que vendem a promessa de uma saúde melhor, mas que não encontraram ainda um ambiente regulatório adequado para conformar suas práticas à necessária proteção dos usuários desses serviços digitais.

Finalmente, a vulnerabilidade digital em saúde está cada vez mais associada à fragilidade dos cidadãos em geral com relação ao recebimento direto, em seus dispositivos móveis digitais, de *fake news* (notícias falsas, mentirosas) relacionadas à saúde. Ultimamente, as *fake news* em saúde vêm provocando impactos individuais e coletivos visíveis no que se refere à vacinação obrigatória no país, mas não só. No Brasil, os efeitos das *fake news* em saúde ao longo da pandemia foram devastadores – da cloroquina passando pelas máscaras até chegar às vacinas. Assim como é muito comum atualmente a circulação de notícias falsas (positivas ou negativas) sobre um determinado produto, um determinado local ou um determinado serviço de saúde, gerando danos e riscos à saúde individual e coletiva de difícil dimensionamento.

No campo da saúde, é bastante comum que políticas públicas de saúde organizadas pelo Estado cuidem de forma diferenciada dos grupos sociais em condição de vulnerabilidade. O conceito de vulnerabilidade vem sendo estudado e trabalhado por diversos autores, em uma constante busca por sínteses conceituais e diretrizes

práticas para a transformação das dimensões comportamentais, sociais e político-institucionais. A vulnerabilidade digital é uma nova forma de vulnerabilidade, e ela deve ser trabalhada para que se entendam as diferentes suscetibilidades de indivíduos e grupos populacionais aos meios digitais. Essas suscetibilidades, agravadas pelos altos riscos dos meios digitais, podem ser fontes de doenças e agravos à saúde com consequências indesejáveis, tais como sofrimento, limitação e morte. Assim, às tradicionais vulnerabilidades que o setor de saúde já é obrigado a cuidar tradicionalmente somam-se as vulnerabilidades digitais, resultantes das novas interações digitais a que estamos sujeitos em nosso dia a dia e, principalmente, as decorrentes dos produtos e serviços de saúde que se utilizam de meios digitais para serem vendidos, disponibilizados e publicizados.

Quando se trata de pessoas em condição de vulnerabilidade na área da saúde, tradicionalmente dois grupos são identificados: a vulnerabilidade por condições de saúde, que afeta aqueles que por alguma condição biológica ou do ciclo de vida necessitam de um cuidado mais específico; e as vulnerabilidades socioeconômicas e culturais, oriundas da condição de vida de um determinado grupo e/ou indivíduo, condição esta que torna esse grupo/indivíduo mais fragilizado socialmente e dependente de tratamento diferenciado por parte do Estado e do sistema público de saúde.

No campo da saúde digital, essas vulnerabilidades são ainda mais potencializadas e conferem fragilidade aos usuários de *sites* e aplicativos de saúde, gerando especial impacto à saúde dos cidadãos que vivem em contextos socioetário, econômico e cultural mais precários e complexos. Esse caldo de vulnerabilidades clássicas associado à vulnerabilidade digital agrava ainda mais os desafios brasileiros no que se refere à promoção da equidade no campo da saúde.

Hoje no Brasil muito se discute sobre as iniquidades de saúde que atingem principalmente os grupos/indivíduos em condição de vulnerabilidade socioetária, econômica e cultural. A análise de alguns indicadores demográficos e sociais do país nos permite perceber claramente essas iniquidades e antever os perigos que esses grupos estão correndo nessa nova era da saúde digital.

Após o escândalo do uso de dados recolhidos no Facebook pela Cambridge Analytica em 2014-2015, influenciando as eleições norte-americanas daquele período, ficou evidente o uso maléfico que os grandes conglomerados digitais do mundo podem fazer com esses dados, como também de que forma isso pode impactar comportamentos e escolhas individuais/coletivas relacionadas

à democracia e, evidentemente, à saúde. A forma como a Cambridge Analytica usou e tratou os dados de milhões de usuários do Facebook para induzir de forma perniciosa o comportamento político dos cidadãos norte-americanos é uma pequena mostra do impacto que esse tipo de tecnologia pode ter sobre a saúde individual e coletiva ao redor do mundo.

O lado mais visível do perigo, ou seja, a indução das pessoas em vulnerabilidade digital para o consumo de produtos e serviços de saúde, é apenas um exemplo do potencial de dano iminente que nos espreita. Os dados sensíveis de saúde podem ser usados para diversos fins eticamente delicados e duvidosos, tais como: determinar quem vai ter um emprego ou não com base nas condições de saúde; definir qual o preço que uma pessoa pagará em seu plano de saúde; definir que tipo de condições de saúde serão admitidas nas políticas de imigração entre países; induzir uma pessoa a determinados comportamentos etc.

Tudo isso já está acontecendo. Urge que a sociedade brasileira (e a global) se organize para conter os infinitos riscos que a saúde digital nos impõe e nos irá impor em futuro não tão distante. É nesse contexto que surge a presente publicação, que oferece insumos estratégicos de alta relevância para que possamos compreender o atual estágio da proteção de dados pessoais sensíveis e ultrassensíveis no âmbito do fenômeno da transformação digital dos sistemas de saúde e para que possamos agir de forma preventiva e responsável, garantindo que o uso dessas tecnologias associadas à saúde digital seja de fato benéfico à sociedade e aos indivíduos.

Esta obra enriquece o debate público nacional para o aperfeiçoamento da proteção de dados de saúde no contexto da transformação digital do sistema de saúde brasileiro

Estudo realizado pelo Comitê Gestor da Internet do Brasil[1] demonstra claramente a fragilidade do atual sistema regulatório e de governança de proteção de dados no Brasil. Os dados, relativos a uma ampla pesquisa realizada no ano de 2023, falam por si mesmos: i) apenas 25% das empresas apresentam uma área específica ou funcionários responsáveis pelo tema de proteção de dados pessoais; ii) 30% das empresas têm bases de dados com dados pessoais sensíveis em suas estruturas; iii) somente 29% das empresas apresentam algum tipo de ação de treinamento

1 Privacidade e proteção de dados pessoais 2023: perspectivas de indivíduos, empresas e organizações públicas no Brasil; Privacy and personal data protection 2023: perspectives of individuals, enterprises and public organizations in Brazil. Núcleo de Informação e Coordenação do Ponto BR. São Paulo: Comitê Gestor da Internet no Brasil, 2024 [livro eletrônico].

ou capacitação sobre proteção de dados pessoais e porte desses dados; e iv) apenas 32% das empresas elaboraram um plano de conformidade ou adequação à proteção de dados pessoais; v) somente 20% das empresas contam com canal de atendimento para os titulares dos dados, como endereço de e-mail, website, ou outros canais; e por aí vai.

Fica evidente, assim, a lacuna de regulação e de compreensão, pela sociedade brasileira como um todo, e as possibilidades dos riscos que o ambiente digital traz à proteção de dados sensíveis das pessoas e, pior ainda, dos usos desviados desses dados para fins que não tenham a ver com o interesse público, com a proteção da segurança e da saúde das pessoas ou, ainda, com a proteção da saúde pública nacional e global.

É nesse cenário que desponta a publicação da presente obra, que representa uma contribuição inestimável ao debate público nacional, ao apresentar análises críticas e atualizadas sobre o fenômeno da saúde digital e sobre o uso da IA no campo da saúde, especialmente no que se refere aos seus impactos sobre os direitos e as garantias individuais do ser humano, notadamente direitos associados à proteção da privacidade, intimidade, liberdade, propriedade e saúde física, mental e social.

A obra contribui para o debate público ao abordar temas abrangentes e estratégicos do fenômeno da saúde digital de forma aprofundada e analítica, ao oferecer elementos fundamentais para uma melhor compreensão de aspectos cruciais que estão modelando a forma como essas tecnologias estão ingressando nos sistemas de saúde modernos, tais como: a dataficação da saúde e as suas relações com a agenda neoliberal; a opacidade algorítmica e os desafios persistentes na coleta e no uso de dados pessoais; a proteção de dados de trabalhadores da saúde em plataformas de atendimento médico em saúde digital; o compartilhamento de dados de saúde suplementar e os limites e as possibilidades do Open Health; a governança de dados sobre a saúde como direito humano; a cultura de proteção de dados pessoais, as assimetrias informacionais e as necessidades urgentes; e os riscos e as vulnerabilidades à proteção de dados pessoais em um contexto de digitalização dos serviços de saúde.

Em outra dimensão, igualmente relevante, a obra também traz importantes reflexões sobre as relações diretas e concretas entre os usos já verificados dessas tecnologias digitais e os impactos que elas podem causar sobre os direitos fundamentais do ser humano. Destacam-se, nesse aspecto, os excelentes artigos que tratam de temas essenciais, tais como: a proteção de dados genéticos; os

aspectos de proteção de dados relacionados aos aplicativos móveis orientados para a saúde mental e para o bem-estar psíquico; o impacto concreto do uso indevido de dados de saúde na vida das pessoas; a coleta indevida de dados pessoais sensíveis travestida de benefícios aos consumidores (CPF para desconto?); e a proteção de dados pessoais nos contextos de serviços de saúde digitais.

Fruto da parceria entre o Instituto de Comunicação e Informação Científica e Tecnológica em Saúde da Fundação Oswaldo Cruz (Icict/Fiocruz), o Instituto de Defesa de Consumidores (Idec) e o Intervozes (Coletivo Brasil de Comunicação Social), esta obra contribui de forma efetiva e construtiva para uma transformação digital do sistema de saúde brasileiro justa, igualitária e benéfica à sociedade e aos indivíduos.

Fernando Aith

Professor titular do Departamento de Política, Gestão e Saúde da Faculdade de Saúde Pública da USP – FSP/USP

Diretor-geral do Centro de Pesquisas de Direito Sanitário da USP – Cepedisa/USP

Editor-chefe da Revista de Direito Sanitário da USP

https://doi.org/10.29397/EdicoesLivres/20250101

A datificação da saúde e o neoliberalismo

Sérgio Amadeu da Silveira

Este texto buscará mostrar as bases discursivas que sustentam a penetração acelerada do neoliberalismo na saúde pública com diversas implicações no Sistema Único de Saúde (SUS). Para tal utiliza como objeto principal de análise o documento denominado "Estratégia de Saúde Digital para o Brasil 2020-2028" (Brasil, 2020), lançado em 2020 pelo Ministério da Saúde. A abordagem iniciará com a seleção dos principais elementos discursivos do neoliberalismo. Em seguida, destacará os traços da Estratégia de Saúde Digital (ESD28) que implica ostensivamente a incorporação dos primados neoliberais, colocando em risco a ideia de saúde universal, constitutiva do SUS.

Antes de entrar efetivamente no caminho de pesquisa aqui destacado, é importante situar como o processo de digitalização está dominado atualmente pela datificação. Também é fundamental destacar que a datificação nem sempre atua no sentido da melhoria dos serviços públicos para todas as camadas sociais. Para Mayer-Schönberger e Cukier (2013) a datificação é a transformação da ação social em dados quantificados *on-line*, permitindo rastreamento em tempo real e análise preditiva. Implica não apenas digitalizar procedimentos e processos, mas torná-los quantificáveis, monitoráveis e disponíveis para análises diversas, principalmente estatísticas e probabilísticas.

Há uma confusão induzida entre digitalização e datificação, uma vez que as consultorias e grandes empresas tecnológicas indicam que a conversão do conjunto de fluxos da vida cotidiana em dados resulta da digitalização. Obviamente, essa geração espontânea não existe. A digitalização de um sistema não implica que todos os seus usuários tenham seus dados capturados, armazenados e analisados. Para que isso ocorra é necessário que dispositivos e, em especial, algoritmos de coleta e análise sejam desenvolvidos e aplicados. Ou seja, dados não são naturais, nem brotam das ações. Eles precisam ser criados e dependem de soluções (*hardware* e *software*) de coleta.

Certamente, sem a digitalização, a datificação estaria muito dificultada. Mas para que algo seja expresso em dados, alguém precisará criar esse processo de

conversão. Por exemplo, as teorias psicométricas existem antes das redes sociais. Todavia, era muito difícil entrevistar centenas de pessoas em um cenário pré-internet e pré-redes de relacionamento social. Michal Kosinski, aproveitando as possibilidades de realizar os chamados *quiz* no Facebook, conseguiu obter dados sobre os traços de personalidade dos usuários que preencheram o seu formulário. Kosinski, em seguida, solicitou autorização desses colaboradores para que seu algoritmo de aprendizado de máquina acompanhasse a sua navegação. Criou-se, então, uma série de novos dados sobre o comportamento das pessoas *on-line*, o que permitiu que o algoritmo extraísse padrões. Enfim, dados surgem a partir da criação de instrumentos geradores.

A afirmação de que os dados são naturais ou que estão disponíveis livremente na natureza refletem o interesse das empresas de tecnologia e das plataformas digitais em obtê-los e tratá-los sem entraves regulamentares. A ideia instigante de que os dados são o petróleo do século XXI porta simultaneamente um elemento aceitável e outro profundamente equivocado. Indubitavelmente, podemos concordar que os dados adquiriram o *status* de ativo de grande valor. Todavia, não é possível concordar que seja extraído da natureza como o petróleo. Dados e tecnologias são criações historicamente situadas.

O que nomeamos de dados são informações de variados tipos que foram e são criadas para uma série de finalidades. Bancos utilizam dados para definir modelos de confiabilidade, probabilidade de pagamento de um empréstimo e para estabelecer uma taxa de risco para grupos de clientes, entre outras finalidades. Seguradoras coletam dados para montar os perfis de risco e aprimorar os cálculos atuariais de seus negócios. Redes sociais reúnem dados e monitoram seus usuários para extrair de seu comportamento *on-line* os padrões de atenção, os perfis agrupados por diversos tipos de interesse, cujo objetivo é modular as condutas com fins comerciais, de *marketing* ou para prestação de serviços. Dados sobre o deslocamento das pessoas nas cidades são importantes para formular políticas públicas de transporte urbano. Muitos são os exemplos que seria possível arrolar aqui.

Talvez seja relevante destacar que a chamada Inteligência Artificial (IA) mais bem-sucedida atualmente é a baseada em uma grande quantidade de dados. *Machine Learning*, *Deep Learning*, redes neurais artificiais, são tipos de inteligência de máquina que necessitam de muitos dados para produzir e treinar seus modelos que serão aplicados em diversos dispositivos, do mecanismo de busca do Google até os sistemas de detecção de biometria facial, passando

pelos sistemas de recomendação de diversos serviços de entretenimento *on-line*, entre tantos outros.

Assim, o termo dataficação expressa um conjunto de ações presentes no cotidiano sociotécnico e que atinge o conjunto de pessoas que utilizam as redes digitais e que interagem nos ambientes cotidianos crescentemente dataficados. Contudo, a primazia dos dados e a implementação de modernos sistemas, baseados na coleta e na análise de dados, não trazem apenas consequências positivas. A pesquisadora Virginia Eubanks descreveu no livro *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* os impactos da tomada de decisão automatizada nos serviços públicos dos EUA. A análise de três casos relacionados ao serviço de bem-estar social, ao serviço de apoio à falta de moradia e aos serviços de proteção à criança, demonstra que a dataficação e a automatização podem ser utilizadas para excluir os segmentos mais fragilizados da população.

Eubanks analisa a reforma do serviço de bem-estar social do estado de Indiana e observa a reunião do que considero o sonho neoliberal da implementação de sistemas algorítmicos, ou seja, a definição da automação como meio de reduzir custos e reduzir a base de pessoas beneficiadas com alegações diversas que vão de falta de documentação, fraude até erros grotescos. A pesquisadora descreve o gasto em um contrato de US$1,3 bilhão para privatizar um serviço estatal, inúmeras falhas técnicas e uma série de ações que retiram o acompanhamento humano das comunidades carentes, entre outros esquemas, para reduzir o alcance da política de assistência.

O caso de Sophie Stipes expressa bem os riscos que sistemas algorítmicos e automatizados trazem para os segmentos mais empobrecidos e fragilizados da sociedade. Sophie, menina de seis anos, foi informada que os benefícios do Medicaid[1] que a mantinham viva seriam interrompidos em um mês, pois ela "não cooperou" com a entrega correta dos requisitos necessários. Um pequeno erro no envio dos formulários gerou o bloqueio dos benefícios da menina. Como os pais de Sophie tinham relacionamentos sociais com pessoas de classes médias, eles conseguiram o apoio necessário para garantir que o novo envio da documentação restabelecesse o Medicaid da criança. Eubanks afirma que outros não tiveram a mesma sorte e perderam o apoio social e de saúde. Isso mostra como os neoliberais utilizam a digitalização e a dataficação para reduzir gastos de programas sociais importantes.

1 NE: Medicaid é um programa de saúde social dos Estados Unidos para famílias e indivíduos de baixa renda e recursos limitados.

Os componentes fundamentais do neoliberalismo

O neoliberalismo está longe de ser um conceito ou noção academicamente pacificada. Sua definição não é consensual. Em vez disso, existem inúmeras controvérsias relacionadas à descrição e à identificação do fenômeno. Alguns privilegiam os aspectos econômicos e de gestão de classe (Anderson,1995), outros seus aspectos ideológicos (Wendy Brown, 2019) ou sua definição como um ordenamento político-social muito além dos limites da economia que penetram em diversos terrenos da existência (Dardot; Laval, 2017).

Reconhecendo as dificuldades de lidar com o fenômeno neoliberal, recorro a inspiração foucaultiana vinda das aulas no Collège de France, entre 1978 e 1979, publicadas no livro *Nascimento da biopolítica*. De lá retirarei os traços e elementos que considero fundamentais do neoliberalismo. O primeiro elemento a destacar é que o neoliberalismo tornou-se um modo, uma racionalidade e um estilo de governar para servir às empresas. O objetivo do neoliberalismo é a formatação da sociedade pelo modelo da empresa. Além disso, o Estado deve se tornar uma máquina que visa entregar o máximo de suas operações para as empresas. O neoliberalismo é o governo das empresas e para as empresas.

O segundo elemento é que tudo deve servir à concorrência. O princípio maior do neoliberalismo é o da concorrência, mesmo onde ela não exista, em segmentos do mercado controlados pelos monopólios, oligopólios e monopsônios. Todo monopolista deve agir como se a qualquer momento emergisse um competidor, um concorrente. Desse modo, o neoliberal não se preocupa com a chamada livre concorrência que tanto mobilizava o velho liberal. A capacidade de competir se liga à ideia de que a empresa deve estar apta a vencer os concorrentes. Levando os argumentos da concorrência até o limite das proposições neoliberais, temos a aceitação da concentração de poder econômico, o culto do mais apto e a defesa de que o importante é crescer e inovar o tempo todo, o que gera a derrota ou a aquisição dos menos aptos e dos seus concorrentes.

Ligado ao objetivo primordial da concorrência está a ideia de capital humano. Como todos devem se preparar para ser empresários de si e verdadeiros empreendimentos, nada mais importante que se "capacitar", se capitalizar, como qualquer empresa apta a competir e a derrotar os concorrentes. Assim, se dissemina um tipo específico de meritocracia em que o inaceitável é perder. O velho liberalismo assumia a falha de sua proposição de que bastaria os direitos formais para assegurar a justiça social, quando reconheceu a necessidade de proporcionar o ensino público e gratuito para todos os segmentos sociais. O liberal

reconhecia que sem níveis educacionais mínimos não era possível dizer que todas as pessoas da sociedade tiveram as mesmas condições de evoluir e acumular riquezas. O neoliberal não acredita em princípios de justiça. Sua perspectiva é a do mercado. Preço justo é aquele que as pessoas estão dispostas a pagar.

Por fim, políticas sociais são consideradas pelos neoliberais um despropósito, pois beneficia os que não têm mérito, os que não são mais fortes e mais aptos. Agigantam a máquina do Estado, atrapalham a lucratividade do setor privado e inserem uma lógica de encontrar um equilíbrio completamente instável e não natural, atrasando o crescimento e o progresso que só pode advir da competitividade, da capacidade de vencer a concorrência, enfim, para o neoliberal a desigualdade é a fonte da prosperidade.

A subordinação da saúde universalizada pela "saúde baseada em valor"

Em 2006, Michael E. Porter e Elizabeth Olmsted Teisberg publicaram o livro *Redefining Health Care*, em que buscam apontar as causas do desempenho insatisfatório do sistema de saúde dos Estados Unidos. No decorrer do livro indicam que o caminho para a superação da falta de qualidade, do desperdício e da baixa lucratividade do setor, seria a implantação dos princípios da competição baseada em valor, cuja verificação deve ser dada pelos resultados das ações do sistema.

Porter e Teisberg alegam que a competição das instituições privadas de saúde, dos seguros-saúde, das clínicas e dos hospitais não se estruturou em função dos resultados, nem foi alinhada com o valor dos serviços. O preceito básico que defendem é a implantação na saúde de um novo tipo de competição, em que o resultado será uma soma positiva para todos os participantes, inclusive, os pacientes do sistema. Nesse sentido, é decisivo aumentar a qualidade dos atendimentos, aperfeiçoar a compreensão das necessidades dos pacientes, obter informações indispensáveis para reduzir gastos desnecessários, apostar na ampliação da satisfação com os atendimentos.

Como é perceptível, a lógica da saúde baseada em valor vem da chamada medicina privada e da realidade norte-americana. A ideia da competitividade neoliberal está presente na doutrina que dirige o sistema. Obviamente a doutrina Porter é a doutrina neoliberal aplicada diretamente na saúde. O que se propõe, em última análise, é a redução de custos para os planos privados. Para isso, é preciso mudar a lógica do sistema e implantar a ideia de custo-efetividade. O custo atribuído ao tratamento de um paciente é sustentado no tempo, quais seus desfechos clínicos?

Para aplicar a saúde baseada em valor é preciso obter dados dos pacientes, dos tratamentos, dos insumos, das clínicas, dos hospitais, entre outros. Os dados são vitais para alimentar os modelos de diagnósticos, os modelos de predição e de detecção de possíveis problemas nos pacientes. Nesse contexto, por exemplo, no Brasil, os médicos de família passaram a ser valorizados não porque a prevenção e a atenção básica são fundamentais em uma política de saúde universalizada, mas porque eles permitem realizar a efetiva redução de custos para a medicina privada.

A IA, nome genérico para as atuais práticas de aprendizado de máquina, para redes neurais, para diversas soluções de aprendizado profundo, para a ciência de dados, passou a ser primordial para a expansão dos seguros-saúde, da saúde privatizada. Contudo, não é possível disseminar uma prática discursiva sustentada apenas na redução de custos. É preciso cultuar a eficiência e a eficácia. É preciso enaltecer a melhoria do tratamento para cada paciente-usuário do sistema. Em uma das dezenas de *sites* brasileiros que divulgam a prestação de serviços tecnológicos e de ciência de dados para a saúde baseada em valor, podemos ler um artigo esclarecedor intitulado "Quem senta na ponta paga a conta?":

> O custo é alto e, no último mês, ele subiu em 15,5% para os beneficiários individuais dos planos de saúde. Um movimento previsível dado os aumentos cavalares de insumos básicos para a população. Não podemos negar que vivemos um cenário traumático pós-pandemia, além de incertezas políticas e guerras ao redor do globo, mas esses eventos sem precedentes são apenas a ponta do *iceberg* dos fatores que tornam, hoje, o ecossistema de saúde insustentável.
>
> Culturalmente, estamos inseridos numa sociedade que estimula, há décadas, o consumo desenfreado. Isso cria uma sensação de "quanto mais, melhor". Aplicando à saúde, vemos – de um lado –, pacientes que associam bons atendimentos a muitos exames, procedimentos, quantidade de consultas e especialistas; e, de outro, profissionais sendo remunerados pelo volume de serviço, não necessariamente pela qualidade. (Triágil, 2022)

Parece evidente que para manter viável o negócio da saúde privada é preciso compatibilizar uma população com renda em queda e expectativa de vida em alta com os custos de atendimento completamente otimizados. É preciso aplicar tudo que a tecnologia digital pode oferecer para aprimorar o sistema e gerar lucro. Daí, a saúde baseada em valor.

Estratégia brasileira de saúde digital e doutrina Porter

O Ministério da Saúde lançou a "Estratégia de Saúde Digital para o Brasil 2020-2028". Antes de iniciar a análise do documento em si como portador ou condutor de princípios neoliberais é necessário trazer um importante trecho de sua introdução:

> A Estratégia de Saúde para o Brasil para 2028 (ESD28) procura sistematizar e consolidar o trabalho realizado ao longo da última década, materializado em diversos documentos e, em especial, na Política Nacional de Informação e Informática em Saúde – PNIIS (Brasil, 2015), publicada em 2015 e em revisão em 2020, na Estratégia e-Saúde para o Brasil (Brasil, 2017) e no Plano de Ação, Monitoramento e Avaliação da Estratégia de Saúde Digital para o Brasil (PAM&A 2019-2023), aprovado em 2019 e publicado em 2020 (Brasil, 2020a). A PNIIS estabelece a fundação conceitual para a saúde digital, incluindo a sua relação com outras políticas públicas e de saúde, com o Plano Nacional de Saúde (Brasil, 2016) e com outras estratégias e iniciativas de governo digital. (Brasil, 2020, p. 5)

Tal explanação indica que a penetração do neoliberalismo não se iniciou na gestão de Bolsonaro e Paulo Guedes. Independentemente de buscar as raízes do avanço neoliberal, aqui a proposta é detectar sua inserção definitiva, a partir dos processos de dataficação e utilização de tecnologias de aprendizado de máquina.

As sete prioridades do Plano de Ação descrevem:

> [...] atividades a serem executadas e os recursos necessários para a implementação da Visão Estratégica de Saúde Digital, orientados pelos três eixos de ação (1 – Ações do Ministério de Saúde para o SUS; 2 – Definição de diretrizes para colaboração; 3 – Implantação do espaço de colaboração) e associados a etapas evolutivas. (Brasil, 2020, p. 24).

Essas prioridades seguem a perspectiva da inovação baseada em empresas inovadoras, do livre fluxo de dados dentro do sistema, da redução de custos e do aumento de qualidade dos serviços, a partir do digital na linha da saúde baseada em valor. São elas:

1. Governança e liderança para a ESD.
2. Informatização dos três níveis de atenção.
3. Suporte à melhoria da atenção à saúde.
4. O usuário como protagonista.
5. Formação e capacitação de recursos humanos.
6. Ambiente de interconectividade.
7. Ecossistema de inovação.

Os elementos que articulam as prioridades e os resultados esperados da ESD são dependentes do amplo compartilhamento de dados, se possível em tempo real, dos pacientes ou usuários do sistema, sem restrições para as estruturas privadas, inclusive para os planos e seguros de saúde. Diversos argumentos apontam a necessidade desses dados estarem amplamente disponíveis e interoperáveis para servirem aos usuários do sistema. Todavia, os fluxos de dados sem restrições para todos os agentes do sistema beneficiam principalmente as estruturas privadas que praticam a medicina voltada ao lucro.

Para a implementação de seguros-saúde de baixo valor que possam ser pagos pela classe média baixa, pelos trabalhadores informais e pelas atuais profissões precarizadas, pelos *bikers* e *motoboys* de aplicativos, é necessário a aplicação de modelos probabilísticos e preditivos alimentados por uma ampla e variada quantidade de dados que permitam inserir essas camadas pauperizadas no escopo de lucratividade das empresas de saúde privada. Dados são indispensáveis não somente para melhorar o atendimento do SUS, mas são vitais para apresentar planos de saúde privados com cobertura limitada e demasiadamente discriminatórios.

A ESD fala da necessidade da consolidação de um protocolo para lidar com os dados em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). É preciso frisar que dados de saúde são sensíveis. Mas o documento não enfatiza a necessidade de definir os seus níveis de acesso. Além disso, em situações de desespero, de dor, de fragilidade, a ideia de consentimento do usuário e de seus familiares para lidar com dados extremamente sensíveis parece ser inócua. A assimetria de conhecimento entre as estruturas de saúde e a pessoa que será atendida é gigantesca. Isso é um dos motivos que legitima o questionamento da chamada liberdade de escolha e da duvidosa ideia de que o conhecimento dos preços é condição suficiente para definir as escolhas dos usuários, no caso compradores de soluções para sua própria saúde.

Outro elemento articulador e norteador da ESD é o preceito da "saúde baseada em valor". Sua inspiração é a doutrina Porter, explicada acima, criada para um sistema de saúde completamente privatizado, sem atendimento universalizado, que é o sistema norte-americano. Obviamente, o desmonte do SUS e do setor público de saúde colabora com a ampliação da medicina centrada em planos de saúde pagos. O avanço da saúde privatizada é um bom negócio para as empresas, mas pode ser um péssimo caminho para o país.

> Medir valor em saúde não é uma tarefa trivial, mas tem se beneficiado das novas tecnologias, que empoderam pacientes e comunidades, oferecendo acesso oportuno a informações de saúde, mecanismos de expressão de suas vontades e opções de tratamento e condutas, permitindo assim que as medidas de valor em saúde possam ser exploradas com rigor científico. (Brasil, 2020, p. 110)

Essa cuidadosa prática discursiva não esconde que o equilíbrio da saúde baseada em valor está no tratamento dataficado e na tentativa de predição de todos os elementos do sistema. Aqui é indispensável ressaltar que quando se fala em uso de tecnologias digitais e de inteligência de máquina se está falando do setor privado. A governamentalidade neoliberal não dá ao setor público a possibilidade de desenvolver tecnologias informacionais. Isso é visto como anacrônico. Cabe ao setor público comprar tecnologias e serviços tecnológicos das empresas. A digitalização-dataficada, nesse cenário, sob a ótica neoliberal, nitidamente enfraquece o setor público e beneficia o setor privado.

Quando se analisam as definições presentes no documento sobre a saúde baseada em valor não está suficientemente exposto o que seria o valor para todos os envolvidos no sistema de saúde. Contudo, se observarmos os "benefícios esperados", podemos ver o peso do que os redatores da estratégia queriam enfatizar:

> - modelos de gestão de saúde baseados em valor;
> - redução dos custos para usuários e fontes pagadoras;
> - capacidade de mensuração do valor objetivo e do valor percebido por todos os atores. (Brasil, 2020, p. 111)

O fato é que um sistema privado de saúde é inviável em uma sociedade de baixa renda ou com renda em declínio. Por isso, se espera encontrar um modelo de gestão capaz de calcular riscos, reduzir custos e manter uma cobrança de pagamentos

mensais viáveis para os diversos segmentos da população. Observem que há uma ambiguidade no discurso sobre a finalidade do termo "valor":

> É chegado o consenso de que é preciso inovar para buscar soluções alternativas capazes de incentivar uma prestação de serviços alinhada mais aos anseios e [às] necessidades dos usuários do que à geração de receitas. Estamos diante de um momento em que tanto sistemas de saúde financiados por recursos públicos quanto o setor privado rumam na direção da saúde baseada em valor.
>
> A expansão dos Serviços Integrados da RNDS [Rede Nacional de Dados em Saúde], que trata da capacidade de interoperabilidade das informações coletadas nas unidades de saúde, bem como a incorporação de tecnologias, métodos, modelos e processos inovadores, é a essência das transformações que o mundo vive hoje. A Estratégia de Saúde Digital para o Brasil reforça que o sucesso das iniciativas que visam o fortalecimento da saúde baseada em valor passa pela discussão de inovações tecnológicas, modelos de remuneração alternativos e pesquisa e desenvolvimento voltados à melhoria contínua da qualidade da atenção à saúde e da sustentabilidade do setor. (Brasil, 2020, p. 95)

Essa passagem torna flagrante o peso dos dados para a construção de um processo de sustentação financeira dos serviços privados de saúde. Sem dúvida, o texto fala de setor público, mas o foco da saúde baseada em valor é a otimização da gestão privada em um cenário de competição. Por mais que se tente negar, os fundamentos da "saúde baseada em valor" se assentam na perspectiva de Michael Porter e Elizabeth Teisberg. Por sua vez, esses são assumidamente focados no ordenamento neoliberal do mundo.

Conclusão

A racionalidade neoliberal é a principal racionalidade do sistema capitalista atual. Desse modo, não parece razoável nem factível enfrentá-la. Seu avanço é constante e atinge estruturas e sistemas construídos em outra lógica, como é o caso do SUS, erguido sobre a ideia de que a saúde é um direito e que sua cobertura deve ser universal, independente da capacidade de pagamento das cidadãs e dos cidadãos.

O processo de privatização da saúde conta com muitos agentes. Um deles é a chamada dataficação, uma vez que se dá na lógica de tratamento quase ilimitado de dados para fortalecer "todos os componentes do sistema". Na realidade, a inovação tecnológica que não visa à universalização, aos primados dos direitos sociais, será utilizada para ampliar a segmentação e a microssegmentação da população em camadas de atendimento, conforme sua capacidade de pagamento.

Defender o SUS implica reorganizar as políticas digitais, proteger os dados dos segmentos mais fragilizados e pauperizados da população, utilizar tecnologias de inteligência de máquina para aumentar direitos, reduzir e eliminar discriminações raciais e sociais operadas por sistemas algorítmicos. A interoperabilidade do sistema não implica que os segmentos privados tenham acesso a todos os dados que possam enfraquecer o setor público e debilitar as defesas que pessoas de baixa renda tenham diante das lucrativas e poderosas corporações privadas. É preciso pensar como criar, desenvolver e disseminar tecnologias para fortalecer a saúde pública universal.

Referências

ANDERSON, Perry. Balanço do neoliberalismo. *In:* SADER, Emir; GENTILI, Pablo (orgs.) Pós-neoliberalismo: as políticas sociais e o Estado democrático. Rio de Janeiro: Paz e Terra, 1995, p. 9-23.

BRASIL. Ministério da Saúde. Secretaria-Executiva. Departamento de Informática do SUS. **Estratégia de Saúde Digital para o Brasil 2020-2028**. Brasília: Ministério da Saúde, 2020. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 8 fev. 2024.

BROWN, Wendy. **Nas ruínas do neoliberalismo**: a ascensão da política antidemocrática no Ocidente. Santos: Politeia, 2019.

DARDOT, Pierre; LAVAL, Christian. **A nova razão do mundo**: ensaio sobre a sociedade neoliberal. São Paulo: Boitempo, 2017.

EUBANKS, Virginia. **Automating inequality**: How high-tech tools profile, police, and punish the poor. Nova York: St. Martin's Press, 2018.

FOUCAULT, Michel. **Nascimento da biolítica**: curso dado no Collège de France (1978-1979). São Paulo: Martins Fontes, 2008.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: die Revolution, die unser Leben verändern wird. Munique: Redline Verlag, 2013.

PORTER, Michael E.; TEISBERG, Elizabeth Olmsted. **Redefining Health Care**: creating value-based competition on results. Cambridge: Harvard Business School Press, 2006.

TRIÁGIL. Quem senta na ponta paga a conta? 23 jun. 2022. Disponível em: https://www.triagil.com.br/post/quem-senta-na-ponta-paga-a-conta. Acesso em: 15 jul. 2022.

https://doi.org/10.29397/EdicoesLivres/20250102

Injustiças epistêmicas e opacidade algorítmica: desafios persistentes na coleta e no uso de dados pessoais

Tarcízio Silva

Dataficação e relações epistêmicas de poder

A geração rotineira de dados digitais tornou-se realidade nas últimas décadas graças à convergência de uma série de fatores sociotécnicos. Poderíamos destacar: a) a ampliação do acesso à internet e o aumento do tempo gasto em ambientes *on-line*; b) o barateamento de tecnologias digitais de registro, processamento e visualização de informações para os mais diferentes setores; c) o investimento tecnocientífico empreendido por Estados, setor privado e capital financeiro; d) o reconhecimento político do valor estratégico local e global do manejo de informações; e e) as tendências de plataformização ligadas a lógicas de eficiência, escala e gestão concentrada de infraestruturas de intermediação de valores, serviços e trocas.

Convergindo com a série de fatores acima, pesquisadoras propuseram lentes de análise a partir da dataficação como um paradigma central para o entendimento de ciência e sociedade. A dataficação se refere a como as bases ideológicas, sociotécnicas e políticas, que centram abordagens focadas em dados na interpretação das realidades sociais, modificam e mediam relações de poder que se direcionam de fluxos de mercado a decisões sobre políticas públicas.

Noortje Marres utiliza o conceito de "redistribuição dos métodos" para falar da convergência de transições: de um empiricismo limitado pelas contingências do *Big Data* para uma redistribuição do poder de interpretação social do Estado e da academia para o setor privado (Marres, 2012).

Refletindo sobre a plataformização da comunicação e da esfera pública, Van Dijck denuncia o uso acrítico das mídias sociais como atalho para o estudo científico de comportamentos, opiniões e tendências sociais.

> Quando as agências governamentais e os acadêmicos adotam as plataformas de mídia social como o padrão-ouro para medir o trânsito social, na verdade, eles transferem o poder sobre a coleta e interpretação de dados do setor público para o corporativo. (Van Djick, 2017, p. 50)

A normalização e hipervalorização das plataformas como "infraestruturas digitais que permitem que dois ou mais grupos interajam" (Srnicek, 2017, p. 43) trouxe, de fato, benefícios de comodidade e velocidade de troca de serviços em áreas diversas, como transporte individual, entrega de alimentos, telemedicina, hospedagem e outros. Entretanto, apesar da empolgação inicial por parte da população sobre mais acesso a serviços antes exclusivos, para poucos, as dinâmicas de precarização do trabalho e a erosão de setores locais evidenciaram-se (Grohmann, 2020).

Através da financeirização calcada na especulação em torno do potencial futuro das empresas dataficadas, fatores como a qualidade dos empregos oferecidos e o tipo de processamento de dados de todos os atores intermediados pelas plataformas tornam-se dependentes dos cambiantes modelos de negócio. Uma questão em especial é o valor dos dados para a construção de modelos e para influenciar comportamentos de grupos hipersegmentados. A corrida por datificação de mais esferas da vida humana significa que as grandes corporações de tecnologia, financiadas por capital financeiro, buscam centralizar quatro camadas do mercado de dados. Além da coleta e do armazenamento, do processamento, da análise e da formação de grupos, o objetivo fim é a modulação. Para Sérgio da Silveira:

> [...] nossa sociedade está construindo uma importante inversão nas exigências democráticas das relações de poder. No mundo industrial, era razoável exigir a privacidade para os cidadãos e a transparência para o Estado. No cenário informacional, estamos vivenciando a construção da opacidade legítima para o Estado e para as empresas enquanto se aceita a transparência completa da vida das pessoas. São as razões do mercado. (Silveira, 2017, n.p.)

A datificação, em um panorama caracterizado pelo aprofundamento de explorações de cunho neoliberal, é um projeto atravessado por disputas constantes. Na última década, o amadurecimento do conhecimento sobre os potenciais e os riscos do uso de dados pessoais e sensíveis para fins governamentais e corporativos tem inspirado mecanismos legais, institucionais e sociais de proteção de dados. Legislações específicas, trabalho investigativo e novos desafios para as organizações da sociedade civil surgem das inter-relações entre atores –

empresas, cidadãos, consumidores, legisladores, ferramentas e tecnologias –, em torno da produção rotineira e estratificada de dados.

A proteção de dados e a (in)justiça epistêmica

A proteção de dados pode ser vista como um conjunto de esforços multidisciplinares para o estabelecimento de consensos públicos e políticos sobre a importância do manejo responsável de dados das pessoas em seus múltiplos papéis como os de cidadãos, eleitores, consumidores ou outros. Os processos globais de dataficação, descritos na seção anterior, geraram demandas por instrumentos científicos e legislativos para a proteção de dados, instrumentos objetos de disputas políticas cada vez mais intensas nas últimas décadas.

Inspirada, sobretudo, na General Data Protection Regulation (GDPR), estabelecida na União Europeia, que a influenciou diretamente, a Lei Geral de Proteção de Dados Pessoais (LGPD, lei n. 13.709/2018) estabelece requisitos para o tratamento de dados, conceitua, identifica e estabelece obrigações e possibilidades dos papéis possíveis em relação aos dados pessoais, tais como os próprios titulares dos dados e os agentes de tratamento, em especial os controladores e operadores. De abordagem principiológica, estabeleceu dez princípios direcionadores: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas.

Apesar do posterior reconhecimento em Emenda Constitucional (n. 115) que a proteção de dados pessoais figura entre os direitos e as garantias fundamentais, a efetiva conformação dos agentes de tratamento aos princípios previstos é um processo em mediação pelo potencial de acionamento do aparato jurídico. Questões relevantes ao princípio de não discriminação, por exemplo, são postas em xeque na literatura contemporânea, a exemplo dos limites do consentimento individual (Mendes; Fonseca, 2020) ou da necessidade de revisão humana de decisões automatizadas (Santos, 2021).

A efetiva busca por princípios – tais como: "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" (princípio da necessidade); "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento" (princípio da transparência); e "impossibilidade de realização do tratamento para fins discriminatórios ilícitos

ou abusivos" (princípio da não discriminação) – passa por entender e abordar os atravessamentos que surgem das hierarquias de conhecimento entre os agentes de tratamento e os titulares de dados. Para Mulholland:

> [...] o problema da privacidade hoje é causado pelo conflito consequente da assimetria de poderes existente entre os titulares de dados e aqueles que realizam o tratamento dos dados. Essa assimetria gera um desequilíbrio social que, por sua vez, leva à violação dos princípios da igualdade e da liberdade. Proteger de maneira rigorosa os dados pessoais sensíveis se torna, assim, instrumento para a efetivação da igualdade e da liberdade. (Mulholland, 2020, n.p.)

Em serviços públicos e privados, como os de saúde, temos a intensificação das possibilidades de produção de conhecimento através do processamento de informação em escala, gerando desafios para a proteção e governança de dados pessoais. As dificuldades que trazem limitações de mecanismos, como a anonimização, a desidentificação e os limites do consentimento informado individual "têm cada vez mais valorizado a necessidade da implantação de mecanismos que permitam o maior controle sobre uso que se faz dos dados" (Ventura; Coeli, 2018, p. 2).

Defendemos nesse artigo que o aprofundamento das hierarquias referentes à posse, ao armazenamento, ao processamento e à coleta de dados, em um contexto de hipervalorização das ciências dos dados, cria desenhos nocivos de deslegitimação de conhecimentos individuais e sociais. Para analisar a questão frente ao debate sobre parâmetros de proteção de dados, em especial no campo da saúde, vamos evocar aqui as proposições de epistemologia social sistematizadas pela filósofa Miranda Fricker.

A conceituação de "injustiça epistêmica" é oferecida por Fricker (2007) como "dano a alguém especificamente em sua capacidade de conhecedor". A lente da injustiça epistêmica permite entender danos e vantagens individuais ou coletivas resultantes da distribuição de credibilidade de indivíduos ou grupos na produção e enunciação de conhecimento.

Fricker analisa dois tipos de injustiça epistêmica. A primeira é a "injustiça testemunhal", que ocorre quando o conhecimento válido de indivíduos é ignorado ou posto em xeque devido a sua posição desfavorável na "economia de credibilidade", com frequência resultante da carga identitária de relações de poder em classe, raça, gênero ou profissão. A economia de credibilidade se configura nos cálculos

heurísticos realizados por indivíduos, através da interpretação e construção de marcadores socialmente negociados. Fricker identifica o papel de estereótipos, interpretados de forma neutra, como "associações amplamente aceitas entre um determinado grupo social e um ou mais atributos"[2] (Fricker, 2007, n.p.).

Nessa concepção, estereótipos não são necessariamente negativos e podem, também, apresentar valências contextuais. Um estereótipo pode estar ligado a marcadores que representam em alguma medida presunções sobre conhecimentos, autoridade e credibilidade frequentes no grupo social estereotipado, resultando no que Fricker chama de "poder de identidade": uma "forma de poder social que é diretamente dependente de concepções sociais-imaginativas compartilhadas sobre as identidades sociais daqueles implicados na operação de poder em questão" (Fricker, 2007, n.p.).

O papel desse poder de identidade e a sua mediação de déficits e excessos de credibilidade na atividade testemunhal é componente essencial da lente da teoria para ler as relações epistêmicas.

Em alguma medida, parte dos estereótipos correntes em determinadas sociedades pode exercer funções heurísticas legítimas e ligadas à capacidade do grupo social. Por exemplo, uma pessoa identificada como médica tende a receber merecida credibilidade em seus enunciados sobre cuidados de emergência. Por outro lado, excessos e déficits de credibilidade também podem ocorrer em outros domínios ou em conjunto com outras categorias. A posição de médico, em sociedades na qual a profissão é sobrevalorizada e ligada a comunidades de "elite", pode colocar tais profissionais em posição de excesso de credibilidade em outros domínios. Escolhas eleitorais, por exemplo, em alguns contextos, podem ser influenciadas pelas opiniões de médicos, ainda que essa profissão não se traduza em conhecimentos sobre gestão pública.

Ainda no campo da saúde, o histórico e a reprodução do racismo colocam médicas negras em desvantagem interseccional na profissão. Comumente confundidas ou desacreditadas como médicas (Nós Negros, 2022), elas conhecem o fenômeno descrito por Fricker por fazerem parte de grupos sociais sujeitos a "preconceito de identidade e, portanto, suscetíveis a um déficit de credibilidade injusto, [e que] também tenderão, da mesma forma, a simplesmente não serem solicitados[as] a compartilhar seus pensamentos, seus julgamentos, suas opiniões" (Fricker, 2007, n.p.).

Mesmo dentro de domínios específicos de conhecimento, há diversos tipos de atores em diferentes posições epistêmicas. A relação médico-paciente no espaço

2 Tradução nossa.

clínico é frequente objeto de estudos sobre os desafios da injustiça testemunhal e as suas ligações com identidades sociais. Revisando trabalhos sobre a violência obstétrica e a disparidade entre a analgesia oferecida a mulheres negras e brancas no país, Gabriel e Santos (2020) explicam que:

> As mulheres que são vítimas dos procedimentos descritos neste artigo parecem estar oscilando entre uma vitimização testemunhal, por não terem suas vontades ouvidas ou levadas em consideração, e uma vitimização hermenêutica, por terem sua participação no entendimento das suas experiências menosprezada. Se essa descrição estiver correta, o debate acerca das injustiças epistêmicas parece apresentar ferramentas importantes para uma compreensão mais ampla das questões que dizem respeito a violações de direitos reprodutivos. (Gabriel; Santos, 2020, p. 9)

A "injustiça hermenêutica" é o segundo tipo de injustiça epistêmica conceitualizado por Miranda Fricker. Para a filósofa, a injustiça hermenêutica "coloca indivíduos e grupos em desvantagens quanto a recursos interpretativos coletivos para compreensão das suas experiências sociais" (Fricker, 2007, n.p.). O acúmulo de impactos epistêmicos de opressões econômicas, políticas e raciais em um mundo moldado pelo colonialismo e pela supremacia branca gera diferentes tipos e níveis de injustiça hermenêutica que prejudicam em especial grupos minorizados historicamente.

Marginalização hermenêutica acontece ao menos através de dois processos que prejudicam o conhecimento coletivo. O primeiro é a produção e institucionalização de conhecimento que exclui as experiências e os aprendizados de determinados tipos de sujeitos e grupos sociais. Vistos pelas instituições hegemônicas de conhecimento apenas como objetos de estudo, são desumanizados não só em seus papéis de enunciadores legítimos, mas também como categorias sociais.

O outro processo, em conexão com o primeiro, é a comum falta ou invisibilização de conceitos ou lentes hermenêuticas sobre fenômenos que, não obstante, existem e geram impactos diferenciais. Um dos exemplos elucidadores usados por Fricker foi a elaboração e disseminação popular do conceito de "assédio sexual". O termo, criado para abarcar a noção de investidas sexuais unilaterais indesejadas, não existia antes da década de 1970 em língua inglesa. O papel do patriarcado na produção de conhecimento e consensos sobre justiça prejudicava os recursos hermenêuticos coletivos. Decisões normativas sobre justiça de gênero eram enviesadas, pois as próprias construções intelectuais hegemônicas sobre

gênero eram injustamente influenciadas de forma desproporcional pelos grupos dominantes (Fricker, 2007, n.p.).

No campo da saúde, o centramento epistêmico do racismo eurocêntrico e do patriarcado como sistemas de opressão prejudicaram em muitas medidas o conjunto dos conhecimentos coletivos, nos países afiliados às culturas dos países coloniais, neocoloniais e imperialistas do Ocidente. Quanto à própria construção de tecnologias de mensuração na saúde, a ideia de "correção racial" é comum exemplo sobre a materialização de injustiças hermenêuticas. O trabalho de Lundy Braun (2014) é um exemplo ao realizar a genealogia do espirômetro – equipamento para medir fluxos de inspiração e expiração. A pesquisadora apontou como crenças racistas do período escravocrata sobre diferenças na capacidade respiratória entre pessoas negras e pessoas brancas foi ponto de partida para mensuração diferencial que prejudicou pacientes por décadas.

De modo similar, algoritmos de Inteligência Artificial em áreas que vão de triagem por planos de saúde (Obermeyer *et al.*, 2019) à medição de gravidade de doença renal crônica (Ahmed *et al.*, 2021) limitaram o acesso de pacientes a cuidados adequados. A gestão algorítmica direcionada à eficiência e ao corte de custos reproduziu injustiças epistêmicas que prejudicam não só grupos específicos, mas todo o conhecimento coletivo sobre as matérias em questão. A aplicação da lógica de "correção racial" em dispositivos e cálculos no campo da saúde é criticada por autores que rogam que: "[...] médicos devem distinguir entre o uso de raça em estatística descritiva, onde exerce um papel vital em análises epidemiológicas, e em procedimentos clínicos prescritivos, onde pode exacerbar iniquidades"[3] (Vyas; Eisenstein; Jones, 2020, p. 880).

Injustiça epistêmica, IA e dados pessoais

O cruzamento de dados e informações para tomada de decisões automatizadas e semiautomatizadas através de aplicações de IA, em especial abordagens opacas de aprendizado de máquina, traz desafios para políticas públicas (Cunha; Barros; Pereira, 2020; Silva, 2021), com desenhos particulares em estruturas híbridas, como a gestão da saúde.

Para Frank Pasquale (2015), a opacidade é uma das características típicas de uso problemático de IA pelos setores privado ou estatal, na medida em que não só impede o controle social da tecnologia, como também desloca a normalização do conhecimento em prol de sistemas aparentemente inescrutáveis. Através

3 Tradução nossa.

de recursos argumentativos e legais como "segredo de negócio", métodos proprietários, termos de confidencialidade ou inexplicabilidade de modelos de aprendizado de máquina, a normalização de decisões opacas traz ameaças de "minar a abertura de nossa sociedade e a justiça dos nossos mercados"[4] (Pasquale, 2015, p. 5).

A transição para uma concepção de IA baseada em modelos de grande complexidade, treinados em bases de dados de escala gigantesca, gerou avanços técnicos que dominaram o campo. No modelo conexionista de IA, caracterizado pelas abordagens de aprendizado de máquina e aprendizado profundo que ganharam primazia no campo nos últimos quinze anos, os novos métodos provaram ser mais efetivos ao mesmo tempo que cada vez mais ininteligíveis (Cardon *et al.*, 2018).

O alvo do cálculo nos sistemas se desloca para o mundo externo ao modelo que lhe fornece exemplos "etiquetados" ou "classificados" de pequenos traços ou sinais em prol do objetivo do sistema algorítmico. Na medida em que o sistema aprende e se adapta sobre a relação entre os sinais e os objetivos, o próprio programa de decisões sobre os dados "evolui" continuamente, de acordo com os objetivos dos desenvolvedores. As abordagens do tipo são louvadas por especialistas tecnicistas no campo que defendem que o conhecimento pode ser gerado:

> [...] automaticamente a partir dos dados, substituindo programadores por sistemas de aprendizado. Este é o nicho do aprendizado de máquina, e não se trata apenas de que os dados continuamente cresceram nas últimas duas décadas, mas também que a teoria sobre aprendizado de máquina para transformar estes dados em conhecimento avançou significantemente. (Alpaydin, 2016, n.p.)

Entretanto, quando se trata de dados e decisões sobre humanos, as próprias conceituações em torno de objetivos definidos, métricas de eficiência, graus aceitáveis de precisão ou impactos nocivos são questionadas. Em campos variados, como medicina (Ferryman; Pitcan, 2018), segurança pública (Benjamin, 2020) e comunicação (Noble, 2018), a mediação algorítmica de gestão de fatos e conhecimentos tem sido paulatinamente investigada com abordagens que envolvem em alguma medida as lentes da injustiça epistêmica.

Injustiças testemunhais mediadas por tecnologias digitais são registradas na implementação de tecnologias de categorização ou identificação de indivíduos

4 Tradução nossa.

até níveis extremos, como o da própria autodefinição pessoal. Dois casos particularmente incisivos podem ser citados abaixo sobre injustiça testemunhal e injustiça hermenêutica propiciados pela mediação algorítmica de conhecimento baseada em dados sociais.

O uso de reconhecimento facial para fins de segurança pública cresceu imensamente nos últimos anos devido a uma interseção de barateamento das tecnologias, a ampliação das bases de dados e o avanço de discurso punitivista na política (Melo, 2021). Apesar da imprecisão, ineficiência e inadequação da tecnologia, atestada tanto por estudos técnicos quanto por campanhas da sociedade civil (Silva, 2022), o reconhecimento facial no espaço público tem sido implementado no mundo a despeito de seus frequentes erros.

Em alguns dos casos de falsos positivos registrados por jornalistas e pesquisadores, temos exemplos de injustiça testemunhal entre cidadãos, agentes de segurança e tecnologia. Um dos casos de maior visibilidade foi a prisão ilegítima de Robert Williams, abordado por policiais em sua casa, na frente da família, acusado de roubar uma loja de relógios em Detroit, EUA. Os policiais chegaram a seu nome e endereço ao rodar uma imagem das câmeras de segurança, na base de dados de reconhecimento facial do departamento. Sua esposa perguntou ao policial para onde ele estava sendo levado e recebeu a ríspida resposta: "Procure no Google".

Na delegacia, Williams precisou mostrar repetidamente aos policiais o quanto a foto do homem nas imagens da câmera de segurança em nada se parecia nem com ele nem com a sua foto da base de dados. Apesar disso, os policiais custaram a questionar a autoridade do sistema computacional. Williams precisou pagar fiança, depois de ter ficado trinta horas preso injustamente, e enfrentou problemas familiares, pessoais e psicológicos pelo ocorrido (Hill, 2020). Casos similares abundam graças a inter-relação entre punitivismo, racismo estrutural e tecno-solucionismo.

O papel do reconhecimento facial nos espaços públicos ao promover excessos policiais e violência estatal que performam também injustiça testemunhal tem sido documentado em relatórios em torno do mundo (Catalano, 2020; Alsur, 2021; Datysoc, 2022; Nunes; Silva; Oliveira, 2022). Estudos densos realizados durante implementações de reconhecimento facial no espaço público puderam descobrir que a influência da cultura policial levou oficiais a priorizar intervenção em detrimento dos procedimentos deliberativos sobre abordagem (Fussey; Murray, 2019).

Se o uso de IA na segurança pública tem o potencial nocivo mais explícito, por ser diretamente letal, a promoção acrítica do uso de modelos de aprendizado

de máquina baseados em treinamento realizado em grandes bases de dados malcuradas traz escala para as injustiças hermenêuticas. O escrutínio de recursos em escala para desenvolvimento de IA, baseada em *Big Data* proveniente de coleta massiva e não curada de dados, evidenciou riscos de reprodução de desinformação sobre o mundo.

Considerada um marco no desenvolvimento de métodos de redes neurais para IA, a base de imagens abertas ImageNet possibilitou a evolução técnica da visão computacional através do compartilhamento de milhões de arquivos de imagens etiquetados com categorias com a pretensão de, literalmente, "mapear completamente os objetos do mundo" (Gershgorn, 2017, n.p.). A base de imagens tornou-se *benchmark* para treinar e medir precisão de modelos de visão computacional e de identificação de objetos e características em imagens, mas foi criticada por limitar "significados potenciais, questões irresolvíveis e contradições. Ao tentar resolver essas ambiguidades, as etiquetas da ImageNet frequentemente comprimem e simplificam imagens em banalidades inexpressivas"[5] (Crawford; Paglen, 2019, n.p.).

Para além da hipersimplificação das visualidades, a base de imagens e os modelos resultantes foram investigados sobre a concentração linguística, geográfica e de gênero sobre sua composição, alimentação e classificação. A coleta inicial de imagens foi realizada apenas em cinco línguas – quatro delas europeias e chinês – e 65% das imagens eram provenientes apenas de cinco países ocidentais, sobretudo EUA e Reino Unido (Shankar *et al.*, 2017). Entre as outras questões apontadas estiveram a misoginia nas etiquetas, que promoveu e invisibilizou dinâmicas violentas de gênero (Crawford; Paglen, 2019; Prabhu; Birhane, 2020), e o próprio trabalho de etiquetagem das imagens, feito por trabalhadores precarizados do Sul Global (Mcquillan; Salaj, 2021) que não se beneficiaram nem financeiramente nem epistemologicamente dos resultados.

Em diversos outros domínios da IA, como o processamento de linguagem natural para fins de identificação de tópicos e moderação de conteúdo, também abundam exemplos de normalização da injustiça hermenêutica. Modelos treinados na coleta indiscriminada e sem curadoria de fontes de dados textuais não estruturados, como notícias, postagens de *blogs* ou até fóruns no Reddit, apresentam problemas de promoção de discurso tóxico contra grupos já vulnerabilizados (Rose, 2022). Entretanto, apesar de não existir "consenso no campo de como e se nós podemos desenvolver sistemas de detecção sensíveis a diferentes contextos sociais e culturais" (Davidson, 2019, p. 9), suas manifestações mercadológicas agem de

5 Tradução nossa.

outro modo, alheias em grande medida aos impactos negativos dos sistemas e em prol das corridas por inovação comercial e normalização dos serviços.

Incidências da injustiça epistêmica no controle social da exploração de dados

Observando a questão da proteção de dados de um ponto de vista coletivo, podemos apontar incidências não plenamente traduzidas ainda em mecanismos de controle e consensos normativos. Lentes de análise que centralizem a justiça epistêmica como meta podem oferecer caminhos para o avanço do debate sobre a adaptação de políticas e compromissos públicos.

A) A proliferação de "duplos" estatísticos

Os processos de identificação individual e coletiva para modelagem de comportamentos e predições sobre resultados fazem multiplicar o que se chama de "duplos estatísticos". A proliferação de ambientes digitais *on-line* e de coleta de dados por instituições de Estado e organizações do setor privado resulta na produção de perfis múltiplos e distribuídos de cidadãos que, apesar de serem inerentemente incompletos, exercem impactos materiais no acesso a recursos, serviços ou direitos.

Os usos e desusos dos duplos estatísticos, sua "correspondência a quem nós somos e o que sabemos sobre nós, os direitos e deveres que temos sobre eles são uma nova área de pesquisa na qual considerações sobre injustiça epistêmica são centrais"[6] (Origgi; Ciranna, 2017, p. 308). Uma cisão fundamental que retira do indivíduo muito de sua capacidade de autodefinição está no fato de que a produção de categorias sobre si prescinde de sua anuência plena e informada para produzir efeitos.

Possibilitadas pelo extrativismo digital, as categorias preditivas permitem que organizações estabeleçam a gestão dos dados pessoais visando ao encaixe em processos algorítmicos direcionados aos resultados. A diluição da autonomia individual através da perfilização, por ser cada vez mais baseada em correlações, ao invés de modelos simbólicos explicáveis, é moeda de troca para otimização das métricas em escala.

O *gap* entre desenvolvimento de modelos e sistemas algorítmicos e sua avaliação ou auditoria (Epstein *et al.*, 2018) parece ser um entrave para a participação social

6 Tradução nossa.

e o escrutínio público essenciais para construção de uso de recursos tecnológicos, como os Sistemas de Informação em Saúde (SIS) (Fornazin, 2020).

B) Múltiplas fontes de vieses

A crença no caráter universal do *Big Data* como representação racional da realidade (Silveira, 2017) é promovida para produzir consensos sobre noções de aplicação ótima dos dados e de sua reprodução em modelos de *entradas* e *saídas* automatizáveis. É a imersão nesse panorama de produção social de ignorância sobre os vieses e problemas dos dados, os modelos e as aplicações que permite a normalização do processamento de dados pessoais, mesmo com a profusão de erros e decisões ocultas.

Sistematizar fontes de vieses tem sido tarefa de pesquisadores, desenvolvedores e auditores interessados em mitigar possíveis danos da IA (Simões-Gomes *et al.*, 2020), em especial abordagens baseadas em dados como o aprendizado de máquina. A proposta de Hovy e Prabhumoye (2021) identifica cinco fontes de vieses no processamento de linguagem natural: a) os dados; b) o processo de anotação; c) as entradas de representação; d) os modelos; e e) o desenho da pesquisa. Para os autores, em alguma medida, todas as etapas na produção de um sistema algorítmico baseado em dados podem incluir vieses que "podem exercer severas consequências e exacerbar desigualdades existentes entre os usuários"[7] (Hovy; Prabhumoye, 2021, p. 4).

Não só a gestão transparente e os mecanismos de supervisão e prestação de contas em cada uma das etapas se tornam necessários para o combate à reprodução de desigualdades. O reconhecimento de iniquidades invisibilizadas através das relações epistêmicas de poder é também ferramenta central para identificação de riscos e mitigação de danos em sistemas baseados em dados. A revisão do campo da IA na saúde demonstra disparidades na produção de dados quanto a especialidades, gênero, nacionalidade e *expertise* (Celi *et al.*, 2022). Merece destaque a escala do estudo realizado por Obermeyer e colaboradores (2019) sobre algoritmos comerciais de predição de necessidades de cuidados médicos, que provou que milhões de pacientes negros receberam atribuição de escores de risco que os prejudicava. Em determinados escores de riscos atribuídos aos avaliados em triagens médicas, pacientes negros estavam, na verdade, muito mais doentes do que os pacientes brancos – e em índices alarmantes.

7 Tradução nossa.

Ao investigar a origem da disparidade na base de dados, os pesquisadores descobriram que os dados que alimentavam o sistema estavam absurdamente enviesados: direta ou indiretamente, atores do sistema de saúde atribuíam menos recursos a pacientes negros. Como a métrica de custo foi aplicada acriticamente, como um *proxy* para supor a condição real dos pacientes, o que o algoritmo fez foi reproduzir, intensificar e esconder as decisões racistas individuais ou institucionais nas clínicas e nos hospitais fontes de dados para o sistema. Como mitigação, os pesquisadores apontam que é necessário um "profundo entendimento do domínio, a capacidade de identificar e extrair elementos relevantes dos dados e a capacidade de iterar e experimentar"[8] (Obermeyer *et al.*, 2019, p. 452).

A negligência dos provedores e hospitais particulares de saúde que usaram o sistema algorítmico para otimizar custos, sem exigir auditorias prévias de impacto potencial, é uma instância de injustiça epistêmica ligada a excessos injustos de credibilidade, uma vez que deveriam ser conscientes da fatualidade discriminatória na saúde pública. A negação dos impactos dos aspectos do racismo em instituições é reforçada pois a "ausência de recursos sociais e epistêmicos muitas vezes só pode ser identificada e medida por aqueles indivíduos e comunidades marginalizados que sofrem com sua ausência"[9] (Carel; Kidd, 2017, p. 341). A construção de sistemas que não levaram em conta vieses multidimensionais ligados às incidências estruturais de discriminação de raça, gênero, classe ou capacitismo gerou o impacto contra os pacientes negros que, paradoxalmente, jogou luz sobre as disparidades de acesso.

C) Contestação limitada

Por fim, e à guisa de conclusão, considerações sobre o avanço da inteligibilidade da sociedade. Modelagens opacas, em sistemas baseados no processamento de dados, promovem "considerações injustas ou inadequadas" combinadas "com o poder dos algoritmos para criar as falhas que alegam apenas predizer"[10] (Pasquale, 2015, p. 216). Ao menos três níveis de relações mediadas por sistemas algorítmicos podem gerar entraves a direitos de contestação de decisões automatizadas por cidadãos.

Destacamos o primeiro que é a própria falta ou o desconhecimento de recursos epistêmicos, muitas vezes ausentes para os próprios atores que usam as implementações em jogo. A definição de métricas, conceitos ou categorias, aplicadas aos indivíduos e grupos, ainda que tenham caráter performativo para

8 Tradução nossa.
9 Tradução nossa.
10 Tradução nossa.

realizar efeitos de ordenação, não são necessariamente explícitas para os sujeitos. O conhecimento de informações básicas sobre o funcionamento dos sistemas frequentemente não é considerado como componente do consentimento para o processamento de dados. Entretanto, por serem implementados como mandatórios para acesso a recursos e serviços essenciais, cidadãos em vulnerabilidade não possuem, de fato, a capacidade de negar o consentimento.

Em estreita relação com o fator anterior, o segundo nível é a hipervalorização das decisões automatizadas tidas como melhores, por suposta neutralidade ou cientificidade "matemática", que favorece injustiças testemunhais contra interpretações das partes vulneráveis na interação. A dataficação, como mecanismo também ideológico, que interage com as vulnerabilidades sociais, em países como o Brasil, leva à percepção pública de que não há caminhos ou, ao menos, não vale a pena o esforço de remediação, o que "pode tornar o indivíduo incapaz de contestar e assim ameaçar sua proteção legal no Estado de Direito"[11] (Hoven, 2021, p. 12).

Por fim, os ideais de produção de sistemas algorítmicos tratam sobretudo de escala e automatização com o fim implícito de corte de custos de recursos humanos. Tendências de autogestão dos serviços, que vão de *chats conversacionais* a interfaces restritivas, são postas em circulação para restringir a capacidade de usuários dos sistemas de contestarem imediatamente e dialogicamente enganos ou erros. A contestação ou revisão de decisões automatizadas, que segue ainda controversa nos instrumentos jurídicos e institucionais em torno do mundo, requer esforços de defesa do seu papel na justiça epistêmica e material.

Referências

AHMED, Salman *et al.* Examining the potential impact of race multiplier utilization in estimated glomerular filtration rate calculation on African-American care outcomes. **Journal of General Internal Medicine**, v. 36, n. 2, p. 464-471, 2021. DOI: 10.1007/s11606-020-06280-5. Disponível em: https://pubmed.ncbi.nlm.nih.gov/33063202/. Acesso em: 15 fev. 2024.

ALPAYDIN, Ethem. Machine learning: the new AI. Cambridge: MIT Press, 2016.

ALSUR. **Reconhecimento facial na América Latina**. Tendências na implementação de uma tecnologia perversa. [Relatório de pesquisa]. 2021. Disponível em: https://www.alsur.lat/sites/default/files/2021-10/ALSUR_Reconocimiento%20facial%20en%20Latam_PR_Final.pdf. Acesso em: 15 fev. 2024.

11 Tradução nossa.

BENJAMIN, Ruha. Retomando nosso fôlego: e*studos* de c*iência* e t*ecnologia*, t*eoria* r*acial* c*rítica* e a imaginação carcerária. *In*: SILVA, Tarcízio. (Org.). **Comunidades, algoritmos e ativismos digitais**: olhares afrodiaspóricos. São Paulo: LiteraRUA, 2020.

BRAUN, Lundy. **Breathing race into the machine**: The surprising career of the spirometer from plantation to genetics. Minnesota: University of Minnesota Press, 2014.

CARDON, Dominique. **Con qué sueñan los algoritmos**: Nuestra vida en el tiempo del big data. Madrid: Dado Ediciones, 2018.

CAREL, Havi; KIDD, Ian James. Epistemic injustice in medicine and healthcare. *In*: KIDD, I. J.; MEDINA, J.; POHLHAUS JR., G. (Orgs.). **The Routledge Handbook of Epistemic Injustice**. Londres: Routledge, 2017.

CATALA, Amandine. Democracy, trust, and epistemic justice. **The Monist**, v. 98, n. 4, p. 424-440, 2015. DOI: https://doi.org/10.1093/monist/onv022. Disponível em: https://academic.oup.com/monist/article-abstract/98/4/424/2563424. Acesso em: 3 fev. 2024.

CATALANO, Andrea. Reconocimiento facial: ¿la brecha entre prófugos capturados y personas con derechos vulnerados justifica su funcionamiento?. **iProfessional**, 2 jan. 2020. Disponível em: https://www.iprofesional.com/tecnologia/305813-Reconocimiento-facial-entre-un-9-de-capturados-y-un-4-con-derechos-vulnerados. Acesso em: 2 fev. 2022.

CELI, Leo Anthony *et al.* Sources of bias in artificial intelligence that perpetuate healthcare disparities – a global review. **PLOS Digital Health**, v. 1, n. 3, p. e0000022, 2022. DOI: https://doi.org/10.1371/journal.pdig.0000022. Disponível em: https://journals.plos.org/digitalhealth/article?id=10.1371/journal.pdig.0000022. Acesso em: 15 fev. 2024.

CHIN-YEE, Benjamin; UPSHUR, Ross. Three problems with big data and artificial intelligence in medicine. **Perspectives in Biology and Medicine**, v. 62, n. 2, p. 237-256, 2019. DOI: 10.1353/pbm.2019.0012. Disponível em: https://pubmed.ncbi.nlm.nih.gov/31281120/. Acesso em: 5 fev. 2024.

CRAWFORD, Kate; PAGLEN, Trevor. **Excavating AI**. The politics of images in machine learning training sets. 2019. Disponível em: https://www.excavating.ai/. Acesso em: 3 jan. 2021.

CUNHA, F. J. A. P.; BARROS, S. S.; PEREIRA, H. B. de B. (Orgs.). **Conhecimento, inovação e comunicação em serviços de saúde**: governança e tecnologias. Salvador: EDUFBA, 2020. Disponível em: chrome-extension://

efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.ufba.br/bitstream/ri/32104/1/CIC-saude-governanca-miolo-ri.pdf. Acesso em: 20 jan. 2024.

DATYSOC. Uso policial del reconocimiento facial automatizado en Uruguay. 23 mar. 2022. Disponível em: https://datysoc.org/2022/03/23/uso-policial-del-reconocimiento-facial-automatizado-en-uruguay/. Acesso em: 15 dez. 2023.

DAVIDSON, Thomas *et al.* Racial Bias in Hate Speech and Abusive Language Detection Datasets. **Association for Computational Linguistics**, ago. 2019, p. 25-35. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://aclanthology.org/W19-3504.pdf. Acesso em: 5 jan. 2024.

EPSTEIN, Ziv *et al*. Closing the AI knowledge gap. **Arxiv**, 2018. Disponível em: https://arxiv.org/abs/1803.07233. Acesso: 1 fev. 2024.

FERRYMAN, Kadija; PITCAN, Mikaela. Fairness in Precision Medicine. **Data & Society at 10**, Report, 26 fev. 2018. Disponível em: https://datasociety.net/library/fairness-in-precision-medicine/. Acesso em: 20 maio 2021.

FORNAZIN, Marcelo. Os desafios da participação nos Sistemas de Informação em Saúde. *In*: CUNHA, F. J. A. P.; BARROS, S. S.; PEREIRA, H. B. de B. (Orgs.). **Conhecimento, inovação e comunicação em serviços de saúde**: governança e tecnologias. Salvador: EDUFBA, 2020. p. 175-194. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://repositorio.ufba.br/bitstream/ri/32104/1/CIC-saude-governanca-miolo-ri.pdf. Acesso em: 15 jan. 2024.

FRICKER, Miranda. **Epistemic Injustice**: Power & the Ethics of Knowing. Nova Iorque: Oxford University Press, 2007.

FUSSEY, Peter; MURRAY, Daragh. Independent report on the London Metropolitan Police Service's trial of live facial recognition technology. Project Report. University of Essex Human Rights Centre, 2019. Disponível em: https://repository.essex.ac.uk/24946/. Acesso em: 20 jan. 2024.

GABRIEL, Alice de Barros; SANTOS, Breno Ricardo Guimarães. A injustiça epistêmica na violência obstétrica. **Revista Estudos Feministas**, Florianópolis, v. 28, n. 2, p. e60012, 2020. DOI: https://doi.org/10.1590/1806-9584-2020v28n260012. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.br/j/ref/a/vqSqgYjmywGvy6BHTs4DFjK/?format=pdf&lang=pt. Acesso em: 20 jan. 2024.

GERSHGORN, Dave. The data that transformed AI research – and possibly the world. **Quartz**, 26 jul. 2017. Disponível em: https://qz.com/1034972/the-data-that-changed-the-direction-of-ai-research-and-possibly-the-world/. Acesso em: 2 mar. 2021.

GROHMANN, Rafael. Plataformização do trabalho: entre dataficação, financeirização e racionalidade neoliberal. **Revista Eletrônica Internacional de Economia Política da Informação, da Comunicação e da Cultura**, v. 22, n. 1, p. 106-122, 2020. Disponível em: https://periodicos.ufs.br/eptic/article/view/12188. Acesso em: 20 jan. 2024.

HILL, Kashmir. Wrongfully Accused by an Algorithm. **The New York Times**, 24 jun. 2020. Disponível em: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html. Acesso em: 2 fev. 2022.

HOVEN, Emilie van den. Hermeneutical injustice and the computational turn in law. **Journal of Cross-disciplinary Research in Computational Law (CRCL)**, v. 1, n. 1, 2021. Disponível em: https://journalcrcl.org/crcl/article/view/6. Acesso em: 20 jan. 2024.

HOVY, Dirk; PRABHUMOYE, Shrimai. Five sources of bias in natural language processing. **Language and Linguistics Compass**, v. 15, n. 8, ago. 2021. DOI: https://doi.org/10.1111/lnc3.12432. Disponível em: https://compass.onlinelibrary.wiley.com/doi/full/10.1111/lnc3.12432. Acesso em: 20 jan. 2024.

MARRES, Noortje. The redistribution of methods: on intervention in digital social research, broadly conceived. **The Sociological Review**, v. 60, n. 1, p. 139-165, jun. 2012. DOI: https://doi.org/10.1111/j.1467-954X.2012.02121.x. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-954X.2012.02121.x. Acesso em: 20 jan. 2024.

MCQUILLAN, Dan. People's councils for ethical machine learning. **Social Media + Society**, v. 4, n. 2, 2018. DOI: https://doi.org/10.1177/2056305118768303. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2056305118768303. Acesso em: 20 jan. 2024.

MCQUILLAN, Dan; SALAJ, Ron. Precarious youth and the spectre of algorithmic stereotyping. *In*: **Young people, social inclusion and digitalisation**: emerging knowledge for practice and policy. (Youth Knowledge 27) Council of Europe Publishing, 2021. p. 87-103.

MELO, Paulo Victor. A serviço do punitivismo, do policiamento preditivo e do racismo estrutural. **Le Monde Diplomatique Brasil**, 18 mar. 2021. Disponível em: https://diplomatique.org.br/a-servico-do-punitivismo-do-policiamento-preditivo-e-do-racismo-estrutural/. Acesso em: 2 mar. 2022.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **REI – Revista Estudos Institucionais**, v. 6, n. 2, p. 507-533, 2020. DOI: https://doi.org/10.21783/rei.v6i2.521. Disponível em: https://www.estudosinstitucionais.com/REI/article/view/521. Acesso em: 11 jan. 2024.

MULHOLLAND, Caitlin. O tratamento de dados pessoais sensíveis. *In*: MULHOLLAND, Caitlin (Org.). **A LGPD e o novo marco normativo no Brasil**. Porto Alegre: Arquipélago, 2020.

NOBLE, Safiya Umoja. **Algorithms of Oppression**: how search engines reinforce racism. Nova York: New York University Press, 2018.

NÓS NEGROS. Médicas negras relatam racismo no trabalho. **Uol Notícias**, 15 fev. 2022. Disponível em: https://noticias.uol.com.br/ultimas-noticias/redacao/2022/02/15/medicas-negras-relatam-racismo-no-trabalho.htm. Acesso: 20 jan. 2024.

NUNES, Pablo; SILVA, Mariah R.; OLIVEIRA, Samuel R. de. **Um Rio de câmeras com olhos seletivos**: uso de reconhecimento facial pela polícia fluminense. Rio de Janeiro: CESeC, 2022.

OBERMEYER, Ziad *et al.* Dissecting racial bias in an algorithm used to manage the health of populations. **Science**, v. 366, n. 6464, 2019, p. 447-453. DOI: 10.1126/science.aax2342. Disponível em: https://www.science.org/doi/10.1126/science.aax2342. Acesso em: 20 jan. 2024.

ORIGGI, Gloria; CIRANNA, Serena. Epistemic Injustice: The case of digital environments. *In*: KIDD, I. J.; MEDINA, J.; POHLHAUS JR., G. (Orgs.). **The Routledge Handbook of Epistemic Injustice**. Londres: Routledge, 2017.

PASQUALE, Frank. **The black box society**.: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PRABHU, Vinay; BIRHANE, Abeba. Large image datasets: a pyrrhic win for computer vision? **Arxiv**, 2020. Disponível em: https://arxiv.org/abs/2006.16923. Acesso em: 15 jan. 2024.

ROSE, Janus. Facebook's New AI System has a "High Propensity" for Racism and Bias. **Vice**, 9 maio 2022. Disponível em: https://www.vice.com/en/article/epxeka/facebooks-new-ai-system-has-a-high-propensity-for-racism-and-bias. Acesso em: 14 maio 2022.

SANTOS, Natane da Silva. Lei Geral de Proteção de Dados e os possíveis impactos da não obrigatoriedade de revisão humana de decisões automatizadas. Trabalho de conclusão de curso – Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito. Rio de Janeiro, 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://pantheon.ufrj.br/bitstream/11422/18950/1/NSSantos.pdf. Acesso em: 20 dez. 2023.

SHANKAR, Shreya *et al.* No Classification without Representation: Assessing Geodiversity Issues in Open Data Sets for the Developing World. **Arxiv**, 2017. Disponível em: https://arxiv.org/abs/1711.08536. Acesso em: 20 dez. 2023.

SILVA, Angélica Baptista. Entre médicos e algoritmos: decisões automatizadas em saúde. **Fórum da Internet no Brasil**, 2021. Disponível em: https://bibliotecadigital.acervo.nic.br/items/35349c38-1d6e-4bdd-9bb1-cc045c245208

SILVA, Tarcízio. **Racismo algorítmico**: Inteligência Artificial e discriminação nas redes digitais. São Paulo: Edições Sesc, 2022.

SILVEIRA, Sérgio Amadeu da. **Tudo sobre tod@s**: r**edes** digitais, privacidade e venda de dados pessoais. São Paulo: Edições Sesc, 2017.

SIMÕES-GOMES, Letícia; ROBERTO, Enrico; MENDONÇA, Jônatas. Viés algorítmico – um balanço provisório. **Estudos de Sociologia**, Araraquara, v. 25, n. 48, 2020. DOI: 10.52780/res.13402. Disponível em: https://periodicos.fclar.unesp.br/estudos/article/view/13402. Acesso em: 5 fev. 2024.

SRNICEK, Nick. **Platform capitalism**. Nova Jersey: John Wiley & Sons, 2017.

VAN DIJCK, José. Confiamos nos dados? As implicações da datificação para o monitoramento social. **Matrizes**, v. 11, n. 1, p. 39-59, 2017. DOI: https://doi.org/10.11606/issn.1982-8160.v11i1p39-59. Disponível em: https://www.revistas.usp.br/matrizes/article/view/131620. Acesso em: 5 dez. 2023.

VENTURA, Miriam; COELI, Cláudia Medina. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança. **Cadernos de Saúde Pública**, v. 34, n. 7, p. e00106818, 2018. DOI: https://doi.org/10.1590/0102-311x00106818. Disponível em: https://cadernos.ensp.fiocruz.br/ojs/index.php/csp/article/view/6752/14571. Acesso em: 7 fev. 2024.

VYAS, Darshali A.; EISENSTEIN, Leo G.; JONES, David S. Hidden in plain sight – reconsidering the use of race correction in clinical algorithms. **The New England Journal of Medicine**, v. 383, n. 9, p. 874-882, 2020. DOI: 10.1056/NEJMms2004740. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.nejm.org/doi/pdf/10.1056/NEJMms2004740?articleTools=true. Acesso em: 20 dez.

https://doi.org/10.29397/EdicoesLivres/20250103

A proteção de dados de trabalhadores da saúde em plataformas de atendimento médico em saúde digital

Jonas C. L. Valente

O artigo tem como objetivo analisar as práticas de coleta e tratamento de dados de trabalhadores da saúde em plataformas de saúde digital. O texto se situa no contexto do crescimento dos serviços de saúde intermediados por Tecnologias da Informação e Comunicação (TICs), em especial os de telemedicina. Integram esse universo plataformas que ofertam diferentes serviços remotos e variadas infraestruturas tecnológicas, de consultas a exames etc. As plataformas digitais no campo da saúde digital fazem a intermediação entre oferta e demanda em diversos aspectos. É o caso de pacientes buscando consultas específicas, ou de médicos ofertando receitas de remédios que podem ser adquiridas *on-line*, ou de profissionais da saúde demandando exames. Os serviços de saúde digital também vêm sendo utilizados como recursos para empresas que desejam adquirir soluções para seus trabalhadores de assistência à saúde.

Segundo relatório sobre o cenário da telemedicina no mundo (Mordor Intelligence, 2022), o mercado era avaliado em US$104,4 bilhões em 2022. Até 2027, a projeção da consultoria é que ele poderá chegar a movimentar US$272,7 bilhões. O relatório aponta a pandemia como um fator impulsionador do crescimento das formas de atendimento a distância mediadas por TICs. Outro relatório (Fortune Business Insights, 2020) prevê um crescimento até 2027 com uma taxa média de 25,8% no setor. Conforme a consultoria, tecnologias como Inteligência Artificial (IA), Internet das Coisas – em inglês, Internet of Things (IoT) – e aprendizagem de máquina impulsionam o desenvolvimento dessa modalidade. Por outro lado, limitações de acesso e infraestrutura ainda são desafios importantes para a expansão dessas aplicações.

Estudo da plataforma Doctor.com (2020), realizado em 2020, indicou que metade dos entrevistados utilizou algum serviço de telemedicina nos três meses anteriores. Entre os ouvidos na sondagem, 83% manifestaram interesse em continuar utilizando esses serviços, após o fim da pandemia da covid-19. Entre os

que não fizeram uso dessa modalidade, 58% alegaram ausência de necessidade de procurar um médico, 32% justificaram dificuldade de arcar com os serviços de saúde e 18% associaram a decisão a problemas técnicos e preocupações com segurança ou privacidade. Entre aquelas pessoas dispostas a contratar algum serviço de telemedicina, 69% mencionaram como fatores positivos a facilidade de uso de tecnologias como *smartphones*, 57% disseram que o fariam a partir do conhecimento da oferta desses serviços, 47% buscariam pela possibilidade de agendamento e também 47% pela possibilidade de acesso imediato a uma consulta ou a algum procedimento.

O número do uso de serviços de telemedicina aumentou no mundo 38 vezes em 2021, em comparação ao período pré-pandemia (Bestsennyy *et al.*, 2021). Contudo, os níveis de adoção variam de acordo com as especialidades. Em fevereiro de 2021, as taxas de consultas por telemedicina iam de cerca de 50% na psiquiatria a menos de 10% em áreas como oftalmologia, cirurgia geral e cardiologia. Conforme o mesmo estudo, 58% dos profissionais de saúde ouvidos viam em 2021 a telemedicina mais favoravelmente do que antes da pandemia. Em abril de 2021, 84% dos entrevistados ofertavam algum tipo de consulta virtual. Um outro levantamento global (Cordina *et al.*, 2022) identificou receio de profissionais de saúde com a telemedicina. Enquanto em julho de 2020, 47% dos profissionais ouvidos recomendavam sempre a telemedicina, quando possível, em abril de 2021, o índice caiu 13 pontos, para 34%. Nesse mês, 17% dos consultados optavam somente por consultas presenciais e 45% colocavam as duas possibilidades, mas sugeriam visitas presenciais.

Enquanto pacientes veem a telemedicina como alternativa pela conveniência (60%), no caso dos profissionais de saúde apenas 36% avaliaram esse tipo como mais conveniente do que as consultas pessoais, contra 64% com posicionamento contrário. Segundo a Mordor Intelligence (2022), o Brasil é classificado como país com baixo índice de crescimento dos serviços de telemedicina. Mesmo assim, os números do cenário brasileiro indicam uma ampliação dessa modalidade. A plataforma Conexa Saúde aumentou sua base de usuários em 500 vezes em nove meses em 2020. Em 2020, a Docway já contava com 4,5 mil médicos credenciados em sua plataforma. A plataforma de emissão de receitas Memed saiu de 2,5 milhões de prescrições em 2019 para 1,5 milhão por dia em 2020 (Associação Paulista de Medicina, 2020).

De acordo com a pesquisa TIC Saúde 2021 (Cetic.br, 2021), dos estabelecimentos conectados (98% dos analisados), 26% ofertavam serviços de teleconsultoria (contra 15% em 2019), 20% realizavam monitoramento remoto dos pacientes (contra

5% em 2019), 20% dispunham de telediagnóstico (contra 12% em 2019) e 18% tinham serviço de teleconsulta. A pesquisa Telemedicina no Brasil (Conexa Saúde, 2021), que entrevistou 801 pessoas e 307 médicos, indicou que 72% consideraram essa modalidade uma boa ferramenta para acesso a serviços de saúde. Entre os motivos citados estão o fácil acesso a um especialista específico, o custo menor e o atendimento com acompanhamento de um médico especialista. Em relação aos médicos ouvidos, 60% consideravam ofertar serviços de telemedicina no futuro.

Conforme a Associação Brasileira de Empresas de Telemedicina e Saúde Digital (Saúde Digital Brasil – SDB), entre 2020 e 2021, foram realizadas mais de 7,5 milhões de consultas por 52,5 mil médicos. Segundo o levantamento Demografia Médica no Brasil 2020, o Brasil possuía naquele ano cerca de 500 mil integrantes dessa categoria (Conselho Federal de Medicina, 2020). Ou seja, as teleconsultas já seriam ofertadas por mais de 10% do universo total desses profissionais.

Plataformas digitais na saúde e em outros campos são pontas de lança de um novo paradigma da informação e comunicação calcado pela coleta massiva de dados, pelo processamento inteligente desses registros e pela oferta de serviços e conteúdos personalizados (Valente, 2021). Nesse novo paradigma, os dados se tornaram ativos fundamentais para a construção de perfis de indivíduos e para o seu uso na obtenção de ganhos econômicos e políticos (Silveira, 2017). Os dados de cada usuário de uma plataforma se tornam insumo-chave para o mapeamento da demanda e a elaboração de seus serviços a partir dela. Mas assumem também a condição de uma mercadoria valiosa em acordos de compartilhamento com outras empresas ou até mesmo na venda desses registros. No caso das ofertas de serviço em saúde digital, ocorre não apenas a coleta de dados dos pacientes, como dos próprios trabalhadores. Esses dados são utilizados para vigiar o "desempenho" dos trabalhadores e organizar a outra ponta: os pacientes que buscam atendimento de profissionais. A partir desses registros, as plataformas monitoram o cumprimento de suas regras internas e os critérios para ampliar notas (escores) ou até mesmo punir o trabalhador com a expulsão.

Essa nova frente de coleta se torna relevante uma vez que as plataformas de telemedicina ou saúde digital se tornam uma opção cada vez mais frequente para o acesso a atendimentos em especialidades diversas. Assim, a análise proposta aqui visa mirar a interseção entre saúde digital, trabalho em plataformas e proteção de dados. Para isso, foram selecionadas três plataformas de telemedicina: Doctoralia, Conexa Saúde e Docway. O intuito foi aferir os graus de vigilância e os níveis de respeito à proteção de dados, partindo da literatura sobre o tema e da legislação brasileira, articulando os parâmetros de proteção de dados com o respeito aos

direitos trabalhistas. Para isso, serão examinados: 1) os dados coletados; 2) as finalidades de coleta e o tratamento realizado; 3) o compartilhamento com terceiros; e 4) a adequação aos referenciais do projeto e aos direitos de titulares previstos na Lei Geral de Proteção de Dados Pessoais (LGPD). A investigação será realizada, sobretudo, por fonte documental. Serão analisadas as informações institucionais e as normas internas, como termos de serviço e políticas de privacidade. Será feita simulação de cadastro nas plataformas para identificar os dados exigidos e os modos de funcionamento do gerenciamento de atividades.

1. Saúde digital e proteção de dados

O presente texto propõe uma análise, a partir da interseção entre saúde digital, proteção de dados e trabalho em plataformas. Começamos, portanto, trazendo referências tomadas na presente análise. O diálogo entre saúde e Tecnologias da Informação e Comunicação (TICs) é amplo e vem ensejando uma grande literatura com diferentes terminologias, como saúde digital, telessaúde, telemedicina e e-saúde, além de distintas conceituações e abordagens teórico-conceituais (Icict/Fiocruz; Intervozes, Idec, 2022).

Seguindo a tradição de apontar o uso de tecnologias eletrônicas em setores pelo prefixo "e-", o uso desses meios técnicos na saúde ensejou a adoção do termo "e-sáude". Aragão e Schiocchet (2020) empregam esse termo para designar o uso de TICs nessa área. O termo foi, inclusive, reconhecido e utilizado pela Organização Mundial da Saúde (OMS, 2018). O conceito de e-saúde surge a partir da implantação de tecnologias sem fio no atendimento em saúde (Colussi; Santos, 2018; Batista; 2019).

A inserção de tecnologias sem fio em serviços de saúde também foi discutida a partir dos termos "telemedicina" e "telessaúde". O vernáculo telemedicina foi institucionalizado na lei n. 13.989 de 15 de abril de 2020 (Brasil, 2020), que autorizou o uso desse expediente durante a Emergência em Saúde Pública de Importância Nacional (ESPIN) por conta da pandemia da covid-19. A norma define a prática como "o exercício da medicina mediado por tecnologias para fins de assistência, pesquisa, prevenção de doenças e lesões e promoção de saúde" (Brasil, 2020). Outros autores caracterizam essa modalidade como a oferta de serviços relacionados à saúde com uso de recursos avançados de informática e telecomunicações a distância (Faleiros Júnior; Cavet; Nogaroli, 2020; Schmitz; Harzheim, 2012). Um outro aspecto constitutivo da telemedicina destacado na literatura é o caráter interativo das relações mediadas por tecnologias (Rodrigues *et al.*, 2020).

A Organização Mundial da Saúde (OMS, 2012) adotou conceito análogo de telessaúde, definido como "a utilização, pela área de saúde, de dados digitais que são transmitidos, armazenados e recuperados eletronicamente e que podem ser usados no apoio ao serviço de assistência médica a distância ou em seu próprio local". Caetano e colaboradores (2020) destacam que a telessaúde pode ampliar as possibilidades de atendimento ao permitir que este ocorra a distância, além de permitir o contato e a relação entre profissionais presentes em locais distintos.

Harayama (2020) opta pelo termo "saúde digital". Segundo o autor, essa designação compreenderia um campo marcado pelas práticas e pesquisas do uso de tecnologias digitais na saúde. O conceito de saúde digital iria além do de e-saúde para incluir desenvolvimentos recentes, como o cenário de amplificação da conectividade, a disseminação de dispositivos de conexão (como *smartphones* e relógios) e as tecnologias emergentes como a Internet das Coisas, a IA, a coleta e a robótica. Almada *et al.* (2020) referem que a inovação em saúde digital enfrenta vários desafios éticos, morais e políticos. Um deles, e objeto de preocupação central do presente trabalho, é o da vigilância e da proteção de dados.

Para além da extensa literatura sobre vigilância, privacidade e proteção de dados, vem merecendo atenção o desenvolvimento desses temas na saúde. Colussi e Santos (2018) levantam a preocupação sobre como o uso das tecnologias nas práticas de telemedicina pode provocar riscos à privacidade na relação médico-paciente, na medida em que há uma exposição das informações passadas pelo paciente e essas informações são armazenadas por meio das plataformas de serviços de teleatendimento. Camara *et al.* (2021) ponderam que o compartilhamento de dados pessoais com os provedores de diferentes serviços representa um risco à privacidade, o que vale também para as plataformas de saúde.

2. Vigilância, plataformas e trabalho

A preocupação com as práticas de vigilância e a proteção de dados pessoais não se restringem à prestação de serviços, como os de saúde, a indivíduos. Nas relações de trabalho, esse é um tema que merece atenção há bastante tempo. Bolaño (2000) destaca como, sob o capitalismo, a informação dentro dos locais de trabalho se torna hierarquizada, para servir às lógicas de funcionamento do sistema e de gestão do processo de trabalho. Ampla literatura[12] mostrou como as empresas sob o capitalismo empregaram métodos de monitoramento e controle estrito dos

12 Destacamos os trabalhos de Braverman (1984) e Burawoy (2012).

procedimentos dentro das rotinas produtivas para potencializar a produtividade do trabalho e minimizar o tempo não trabalhado.

Dentro dos limites do presente texto, cabe-nos assinalar as transformações recentes e os novos modos de gestão do trabalho, a partir da plataformização das relações sociais de produção. Plataformas digitais podem ser entendidas como sistemas tecnológicos que agenciam interações, discursos e transações entre indivíduos e organizações (Valente, 2021), incluindo os trabalhadores que colocam sua força de trabalho à venda no mercado e contratantes dessa força de trabalho. As relações sociais de produção que ocorrem em plataformas vêm sendo discutidas na literatura como "trabalho em plataforma" (Daugareilh *et al*., 2019; Rani; Furrer, 2020; Valente, 2021), ou, em termos relacionados, como "trabalho logado" (Huws, 2016) e "uberização do trabalho" (Abílio, 2019). Graham e Woodcok (2020) colocam as "plataformas de trabalho digital" no centro da "economia de bicos" (*Gig Economy*) como novos mercados caracterizados por trabalhadores independentes contratados por meio dessas plataformas.

Definimos aqui o trabalho em plataforma como relações de trabalho operadas no âmbito de plataformas e a partir de regras definidas por elas, sejam com força de trabalho empregada pelas próprias plataformas (como empregados diretos ou indiretos de Facebook, Amazon ou Twitter) ou por força de trabalho agenciada, mediada, por plataformas (como Uber, Workana e Amazon Mechanical Turk).

A despeito de opções distintas para a conceituação, autores convergem na compreensão de que o trabalho em plataforma é marcado por novas formas de controle, por estratégias de gerenciamento, a partir de algoritmos, pelo ranqueamento dos trabalhadores como forma de disciplinamento e por modelos opacos que encobrem os critérios e os modos de operação das plataformas para os trabalhadores. Discutindo os avanços na vigilância do trabalho em plataforma e remoto, Ball (2021) aponta quatro novos desenvolvimentos da vigilância nos locais de trabalho: o aumento do uso de tecnologias que permitem a vigilância para além da gestão dos processos de trabalho; o monitorando de pensamentos, sentimentos, comportamentos; a localização e a movimentação; além do uso de táticas de administração pelos sistemas de reputação e pela avaliação do empregado. Esse cenário foi amplificado durante a pandemia. O trabalho remoto veio acompanhado de novos métodos de monitoramento do trabalho e dos trabalhadores, bem como por uma mistura maior das fronteiras entre tempo de trabalho e tempo privado.

Tanto no trabalho remoto, mas especialmente no trabalho em plataformas, a vigilância se torna mais necessária para o controle do tempo e do desempenho

dos trabalhadores a distância. Tal esforço é ainda maior diante de uma massa de trabalhadores espalhada por diversos locais. Destarte, os requisitos e métodos de coleta de dados assumem papel central para o funcionamento dessas plataformas. Há um primeiro movimento de coleta de dados para identificação do profissional e validação deste e de suas credenciais. Os dados são fundamentais para elaborar o perfil que será exposto para o acesso pelos contratantes. Outra funcionalidade necessária é o controle das atividades realizadas. Tal administração é relevante para quantificar as atividades desenvolvidas no âmbito da plataforma e para calcular a base de remuneração desse agente mediador. Embora haja distintos modelos de negócio, inclusive com pagamento de mensalidades, o arranjo mais comum envolve as plataformas taxando parte das receitas auferidas pelos trabalhadores nas tarefas realizadas.

A coleta de dados é relevante também para a formação de cadastros. A coleta massiva se tornou um traço constitutivo das plataformas digitais e esses registros viram insumos para desempenhar diversas atividades, sejam elas de *marketing* e divulgação dos próprios serviços, sejam outras de compartilhamento mútuo de cadastros com parceiros e terceiros em troca de vantagens ou com vistas a obter ganhos financeiros ou outras formas de compensação.

A coleta de informações dos trabalhadores também é condição necessária para administrar os retornos dos "clientes" que contratam essa tarefa. Assim, a manutenção de parâmetros de qualidade e a resolução de disputas e conflitos no âmbito da execução do trabalho demandam grau significativo de controle. Se tal premissa já se coloca em um ambiente físico com relativo grau de visibilidade (como em um consultório ou hospital), faz-se ainda mais necessário, quando as atividades ocorrem a distância. Os dados são insumos para o monitoramento das transações e interações realizadas no âmbito da plataforma e para o funcionamento do seu gerenciamento algorítmico.

Dessa forma, a privacidade e a proteção de dados ganham contornos especialmente relevantes nas relações de trabalho. Se já são direitos fundamentais da sociedade contemporânea cada vez mais datificada, quando há relações de subordinação os riscos de abusos e de violações desses direitos podem assumir uma condição ainda maior. No cenário do trabalho em plataformas, essa combinação tem potencial de abrir espaço para práticas cada vez mais intensificadas de vigilância. Após a exposição breve de referenciais, o texto avança a seguir para a análise das três plataformas de telemedicina examinadas.

3. Vigilância e proteção de dados em plataformas de telemedicina

A análise tomou como objeto três plataformas de renome nacional: Docway, Conexa Saúde e Doctoralia. As três são plataformas de atuação nacional, com expressão nacional. Embora não haja *rankings* ou levantamentos com *marketshare* sobre o segmento, a seleção tomou como referências a quantidade de usuários, quando informada, e as menções em publicações especializadas.

3.1 Docway

A Docway oferece serviços de telemedicina tanto diretamente para pacientes quanto para empresas que querem adotar esses serviços entre suas políticas de saúde e segurança do trabalho ou como oferta de benefício a seus trabalhadores. São providos serviços de triagem, teleatendimento, acompanhamento por enfermeiros, atendimento presencial, encaminhamento a médicos especialistas e ao pronto-socorro, na modalidade *Fast Track*. Segundo a própria empresa, ela opera com mais de 10 milhões de pessoas, tendo uma carteira de mais de quatro mil médicos, atendendo em 25 especialidades em 26 estados do país.

As regras gerais e de coleta de dados da Docway são definidas em três documentos. Há dois termos de serviço distintos, um para o serviço de pronto atendimento digital (Termos PAD) e outro para o consultório digital (Termos CD). Esse último é o termo de consentimento para a coleta de dados sensíveis de pacientes. Além desses, há uma Política de privacidade (Política) que detalha a coleta, o tratamento e o compartilhamento dos dados dos usuários, entre eles, os profissionais. A plataforma indica que poderão ser elaborados e implementados termos adicionais sobre serviços específicos, que serão divulgados. Contudo, na época da realização dessa pesquisa, não havia nenhum exemplo de termo adicional no *site* da companhia.

A aceitação dos termos é condição para a atuação, a partir da plataforma. Alterações podem ser realizadas sem aviso-prévio, que *poderão* (grifo nosso) ser comunicadas aos profissionais por meio de canais de interação entre os profissionais e a plataforma. Na Política de privacidade, a modificação também é aventada, contudo o texto afirma que essas deverão ser notificadas aos usuários. Nos Termos PAD, é instituída a responsabilidade dos profissionais conferirem periodicamente os termos para monitorar eventuais ajustes. Para atuar na plataforma, o profissional faz um cadastro, que é analisado e precisa ser aprovado pela empresa. A empresa também

possibilita o cadastro de pessoas jurídicas, como clínicas, que terão de registrar seus profissionais na plataforma. Não há responsável oficial indicado no *site* ou na Política de privacidade. Nesse documento, consta apenas um *e-mail* de contato genérico para "dúvidas e preocupações não abordadas" (contato@docway.co).

A empresa Docway define duas modalidades de trabalhadores em seus termos, separando médicos dos demais profissionais de saúde. Os primeiros são caracterizados como "profissionais formados em medicina, devidamente regularizados para o exercício da profissão em sua respectiva especialidade e sujeitos ao Conselho Regional e Federal de Medicina (CRM/CFM)" (Docway, Termos de uso do profissional de saúde), enquanto os segundos abarcam psicólogos, nutricionistas, fisioterapeutas e enfermeiros regularizados para o exercício da profissão e inscritos nos respectivos conselhos.

Quanto à coleta, a Política de privacidade da Docway não detalha nem especifica quais dados são coletados, apenas trata genericamente os dados disponibilizados no cadastro e no uso da plataforma. "Ao registrar ou submeter informação a esse aplicativo, você concorda com a utilização de tais dados, em conformidade com esta declaração de privacidade" (Docway, Política de privacidade). O documento exemplifica tipos de informações que poderão ser solicitadas, entre as quais: "nome, cargo atual, endereço, telefone, entre outros" (Docway, Política de privacidade). Pelos Termos PAD, a empresa informa que pode solicitar informações adicionais para confirmação dos cadastros e identificação dos trabalhadores.

Em relação às finalidades e ao tratamento, a Política de privacidade apresenta de forma extremamente sucinta e genérica as finalidades de uso dos dados coletados de usuários, em geral, sem diferenciação entre pacientes e profissionais, para a operação da plataforma. O documento informa que poderão ser tratados dados para "contabilizações estatísticas Docway ou para personalizar a experiência do usuário em nossos domínios, sem identificação pessoal ou financeira do utilizador" (Docway, Política de privacidade).

Os dados são coletados para as finalidades de prestação dos serviços da plataforma. Contudo, os Termos PAD abrem uma brecha bastante ampla ao preverem que a empresa pode vir a prestar qualquer tipo de serviço. "A Docway poderá oferecer, a seu critério, produtos vinculados ou não ao serviço, bem como poderá prestar outros serviços, gratuitos ou onerosos, conforme acordado com os profissionais" (Docway, Termos PAD).

A Política de privacidade menciona o uso de dados para a finalidade de alimentar serviços de *marketing*. Mas não detalha quais dados podem ser tratados com esse

propósito. "Realizamos nossas atividades de *marketing* em conformidade com a legislação aplicável vigente e garantimos a implementação de procedimentos para obter autorizações necessárias" (Docway, Política de privacidade). Ainda conforme a Política, os usuários podem solicitar a suspensão desses procedimentos por meio de requerimento diretamente à plataforma.

No tocante ao compartilhamento, segundo a Política, os dados só poderão ser vistos pelo usuário, pelos profissionais de saúde e pela equipe da plataforma. Uma exceção é o compartilhamento dos dados dos pacientes com hospitais, quando esses necessitarem de atendimento nessas instalações. O documento também elenca que dados poderão ser fornecidos a instituições públicas e autoridades regulatórias para "aplicação da lei".

3.2 Conexa Saúde

A Conexa Saúde é uma plataforma que oferta serviços para pacientes de consultas a distância em diferentes especialidades, como clínica geral, cardiologia, dermatologia, psiquiatria, neurologia e oftalmologia. São disponibilizados procedimentos como teleconsulta, pronto atendimento virtual, telemonitoramento, teleorientação e "cuidado integrado em saúde". São ofertados serviços para instituições de saúde e também para empresas com foco em atendimento de trabalhadores, com grupos na carteira como Magalu, Unimed, Liberty Seguros e Golden Cross.

A empresa possui em seu *site* uma página específica para assuntos relacionados à LGPD. O Oficial de Proteção de Dados é identificado, seu nome é fornecido, bem como o endereço para contato. Nessa página, são disponibilizados os seguintes documentos: Termos e condições gerais de uso, Consentimento livre e esclarecido (Termos), Política de privacidade (Política), Política de *cookies* para médicos (Política sobre *cookies*). Assim como nos demais casos, os termos informam que a adesão à plataforma implica a aceitação não somente desses como do conjunto das políticas da plataforma.

Podem se cadastrar profissionais cadastrados em conselhos profissionais. Os Termos de uso podem ser alterados em qualquer hora, sem aviso-prévio ou responsabilização diante dos usuários (pacientes e profissionais). O texto prevê que os usuários serão informados por *e-mail* de alterações, mas abre possibilidade de isso não acontecer. Segundo a Política, a mudança pode ser informada também no próprio *site*. A aceitação das políticas e das alterações é mandatória, cabendo ao usuário a desvinculação, caso tenha discordância com o ajuste nas regras.

Nos Termos, os trabalhadores são denominados "profissionais de saúde" e definidos como: "Profissional da saúde regularmente inscrito no seu respectivo conselho e autorizado a oferecer serviços de telessaúde, que deseja utilizar a solução Conexa Saúde e, para isso, concorda com os Termos de uso e demais políticas da plataforma" (Conexa Saúde, Termos e condições gerais de uso). A Política de privacidade repete as definições de dados pessoais e dados sensíveis da LGPD, o que auxilia o usuário a entender melhor as disposições ali presentes.

Quanto à coleta, segundo as Políticas, são coletados os seguintes dados dos profissionais de saúde: a) Nome completo; b) CPF; c) Telefone; d) Endereço de *e-mail* válido; e) Endereço; f) Imagens; g) Áudios; h) Inscrição válida no conselho de representação profissional respectivo (CFM, CFP, CFO, COFEN, CFN, COFFITO, CFFa, CFESS); i) Descrição do currículo; j) Vídeo de gravação da consulta, apenas nos casos em que essa função estiver habilitada; e k) Assinatura via certificado digital ICP-Brasil.

Também são coletados dados definidos na Política como "de utilização": a) Registro de qualquer comunicação realizada entre pacientes e profissionais de saúde; b) Detalhes das visitas à plataforma e dos recursos que o paciente ou profissional acessou; c) Informações do dispositivo de acesso utilizado; d) Informações de *log* de acesso (que incluem IP do dispositivo, data e hora); e) Mapeamento de cliques no navegador, dados de navegação, estatísticos, demográficos, entre outros; e f) Dados preferenciais sobre como o paciente ou profissional de saúde interage com os serviços, as preferências manifestadas e as configurações escolhidas.

Nos Termos, a empresa afirma que utiliza "todos os meios válidos e possíveis" para identificar pacientes e profissionais, podendo requerer informações adicionais e documentos (não discriminados) para essa identificação. A Conexa Saúde utiliza *cookies* funcionais (empregados para operação da plataforma), de desempenho (que fornecem informações sobre como o *site* é utilizado), de sessão (enquanto uma visita ao *site* ocorre) ou outra categoria denominada "persistentes" (que continuam instalados no aparelho do usuário, enquanto não forem deletados).

O uso de *cookies* é condicionado a uma autorização, solicitada e fornecida no próprio *site*. O profissional pode recusar a instalação dos *cookies* em seu computador ou *smartphone*. Nesse caso, a Política informa que poderá haver comprometimento de parte das funcionalidades, mas não detalha quais. Conforme a Política de *cookies*, são utilizados *cookies* do Google (Double Click) e do YouTube. No documento, são expostos os caminhos para recusar a instalação e operação dos *cookies*.

A Política de privacidade disponibiliza uma tabela em que atribui para cada dado ou conjunto de dados as finalidades da coleta e a sua base legal. A grande maioria dos dados pessoais dos profissionais, utilizados com a finalidade de os identificar, é coletada com base na hipótese da LGPD de execução de contrato (art. 7º, V). Outros dados, como *e-mail* e telefone, têm como base o consentimento (art. 7º, I). Já registro legal e *logs* de navegação são coletados na hipótese de cumprimento de obrigação legal ou regulatória (art. 7º, II).

Em relação à finalidade e ao tratamento, na Política, a Conexa Saúde elenca as finalidades do tratamento dos dados pessoais, entre as quais:

> a) realizar identificação e cadastro dos pacientes e profissionais de saúde na plataforma e disponibilizar os serviços; b) garantir que o conteúdo da plataforma seja apresentado da forma mais eficiente para o paciente ou profissional de saúde; c) ajudar a realizar melhorias de caráter geral na plataforma; d) processar os dados colhidos por diferentes algoritmos internos do serviço ou de terceiros; e) realizar e apoiar pesquisas científicas em prol da promoção de estudos em saúde pública, por meio do uso de dados anonimizados e desde que respeitados os devidos padrões éticos relacionados a esses estudos e pesquisas; f) contatar e notificar o paciente ou profissional de saúde acerca de modificações na plataforma, serviços oferecidos pela Conexa Saúde ou em suas políticas e termos de uso, quando necessário; g) analisar as informações fornecidas a fim de garantir uma prestação de serviços efetiva pelo profissional de saúde; h) processar os dados com o fito de auxiliar no controle do absenteísmo nas empresas; i) enviar *newsletters* e correios informativos; h) realizar campanhas de *marketing* e enviar publicidade através dos meios de contato informados; i) realizar cobranças sobre os serviços prestados, quando aplicável. (Conexa Saúde, Política de privacidade)

A empresa utiliza os dados pessoais para envio de mensagens publicitárias. O profissional pode recusar esse tratamento, mas o sistema é de *opt out*, devendo informar a negativa para deixar de receber em vez de a plataforma precisar obter uma autorização para começar a enviar tais comunicados. Os Termos definem que a empresa não se responsabiliza por intermitências ou problemas no funcionamento da plataforma nem por perdas em informações decorrentes dessas dificuldades.

Os prontuários eletrônicos são guardados por vinte anos, seguindo dispositivo da lei 13.787 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.

Informações incorretas ou inverídicas podem ensejar o desligamento do usuário da plataforma. Mas os Termos colocam que também poderá haver uma notificação ao profissional para que esse retifique essas informações. Caso isso não seja feito, a pessoa poderá ser bloqueada. Em caso de acesso indevido ou violação de segurança por parte de um profissional de saúde, ele poderá ser responsabilizado pela plataforma. Os profissionais também ficam proibidos de gravar consultas realizadas por meio da plataforma.

No que se refere ao compartilhamento, a Política estabelece um conjunto de hipóteses e situações de compartilhamento dos dados com terceiros. Isso poderá ocorrer em caso de procedimentos necessários para o cumprimento de obrigações legais, para prevenção de fraudes e outros crimes, em resposta à demanda de uma autoridade competente, se a empresa entender que as solicitações estão de acordo com a lei. A hipótese também será admitida para "proteger direitos, bens ou segurança" da plataforma; para fornecedores ou consultores de *marketing*, *Data Analytics* ou *Business Intelligence* que "precisem" acessar as informações para prover serviços em nome da plataforma; e para órgãos de fiscalização e controle.

O compartilhamento com terceiros também será realizado para finalidades quaisquer, caso o usuário concorde. Desde que obtido o consentimento, a Conexa Saúde poderá compartilhar dados pessoais com outras empresas do seu grupo, para o atendimento das finalidades previstas na Política ou para "continuidade no cuidado integrado de saúde". Relatórios estatísticos com dados anonimizados poderão ser repassados a parceiros e afiliados. Quanto à transferência internacional de dados, a Política afirma que segue a diretriz da LGPD e só compartilha com controladores ou operadores em países que dispõem de níveis de segurança e proteção de dados pelo menos semelhantes aos do Brasil.

A Política também elenca os direitos dos usuários, apresentando aqueles previstos na LGPD. Entre eles, estão: a) confirmação da existência do tratamento; b) acesso pelo titular aos dados que a empresa possui; c) correção de dados pessoais pelo titular; d) exclusão dos dados a qualquer momento, com exceção de necessidade de retenção para cumprimento de obrigação legal; e) oposição ao tratamento em geral e para finalidades de *marketing*; f) de portar os dados e receber uma cópia para uso em outro controlador; g) não se submeter a decisões unicamente automatizadas, caso essa tenha efeito jurídico ou igualmente

significativo; h) solicitar anonimização; e i) restringir o tratamento de todos ou parte dos dados pessoais.

3.3 Doctoralia

Doctoralia também é uma plataforma de telemedicina. Em seu *site* institucional, a empresa afirma dispor de mais de 700 mil profissionais de saúde para atendimento dos pacientes. A empresa disponibiliza tanto opção de atendimento presencial como teleconsulta. Além das possibilidades de teleconsulta, o grupo desenvolve e oferta serviços para clínicas e profissionais autônomos. O *website* apresenta uma seção específica denominada "Segurança de dados", mas com foco no paciente. No caso dos dados dos profissionais, há dois instrumentos reguladores: os Termos de uso (Termos) e a Política de privacidade. A empresa informa na Política que poderá alterá-la, especialmente em decorrência da mudança de seus serviços. Mas não prevê obrigação de informar essas mudanças aos profissionais.

A empresa define o *site* como uma plataforma que "expõe os perfis de profissionais de saúde" e viabiliza "consulta às informações, espaço para avaliação por parte dos usuários e, a depender do contrato do profissional, a disponibilidade de horários para agendamento *on-line* de consultas presenciais e/ou teleconsultas" (Doctoralia). O trabalhador é classificado como "profissional de saúde do perfil básico". Na Política de privacidade, o profissional é tratado como "especialista". As condições para isso são a criação de um perfil e o firmamento de um contrato de prestação de serviços, a partir da aceitação dos Termos. Os termos informam os canais de comunicação com um endereço de *e-mail* genérico e a Política informa em seu início que há um Oficial de Proteção de Dados e disponibiliza seu contato (dpo.br@docplanner.com).

Em relação à coleta, a plataforma utiliza a aceitação dos Termos de uso e condições gerais como atestado de consentimento da política de privacidade. "Ao aderir ao contrato o usuário e os profissionais do perfil básico: consente com o processamento de dados pessoais de acordo com os Termos de uso e em especial a nossa Política de privacidade" (Doctoralia, Termos de uso e condições gerais). O *site* condiciona a revogação do consentimento ao uso da plataforma.

A plataforma coleta dados, mas não somente os fornecidos pelo profissional, ela realiza coletas em bases públicas. "A Doctoralia presta serviços de informação sobre médicos, com base em seus cadastros pessoais realizados ativamente pelo profissional, ou em dados públicos obtidos na rede ou nos conselhos profissionais" (Doctoralia, Política de privacidade). Os profissionais na Doctoralia iniciam com

um perfil básico. Nessa modalidade, é preciso fornecer: título profissional, primeiro nome e sobrenome, endereço e detalhes de contato para o local onde os serviços de saúde são realizados, a especialização do profissional e o(s) número(s) de registro profissional, caso aplicável. Outros dados podem ser requeridos, embora a plataforma nos Termos não especifique quais são.

Na Política, estão listados dados coletados:

> [...] seu nome e sobrenome, seu endereço profissional, seu endereço de *e-mail*, sua especialização, sua educação e informações sobre doenças que você trata ou exames que você realiza, seu número profissional (o número da licença que permite que você realize atividades profissionais), sua imagem, detalhes de clínicas com as quais você colabora, e quaisquer outros dados que você nos forneça durante o processo de registro ou durante a execução de um contrato pago. (Doctoralia, Política de privacidade)

Em pacotes *premium*, também são coletados programação, agenda, serviços prestados, preços desses serviços e meios de pagamento utilizados. A plataforma também pode ter dados de instituições que firmaram contrato com ela. Não são detalhados quais dados. A Política elenca o direito de o profissional solicitar a retirada dos dados compartilhados da instituição (plataforma). A Doctoralia informa que pode coletar dados adicionais, tais como: informações sobre dispositivo, endereço IP, fuso horário e idioma, navegador, localização, quando a pessoa usou os serviços da plataforma pela primeira, última vez e tempo de uso.

A plataforma coleta também dados de profissionais que não se cadastraram nela, por meio de bases como: registros publicados pela pessoa, de médicos, bases públicas de conselhos profissionais e relatos de pacientes do Doctoralia. Entre esses estão: nome(s) e sobrenomes(s), endereço profissional, profissão e/ou especialidade, opiniões dos usuários dos serviços e número de registro profissional. A Política coloca que o profissional pode se opor ao tratamento e requerer a exclusão de seus dados.

A Doctoralia obtém registros também por meio de *cookies*. São empregados *cookies* para armazenamento de dados da conta, *cookies* funcionais para "tornar sua experiência mais amigável", *cookies* de desempenho "para observar como nossos serviços são usados e obter estatísticas do uso", *cookies* de *marketing* e *cookies* "de terceiros". Nessa última categoria, são listados apenas alguns exemplos, como Google Analytics, HubSpot e "botões de mídia social". A Política

indica como é possível desativar os *cookies*, mas alerta que isso poderá afetar as funcionalidades do *site*.

Conforme a Política de privacidade, as bases de coleta de dados dos profissionais são para execução de contrato e para obrigações legais como emissão de notas fiscais e manutenção de registros financeiros atualizados. Quando a finalidade é de *marketing*, esta se encaixa em "outros propósitos" ou é concernente a profissionais não cadastrados, a base legal informada é o legítimo interesse (LGPD, art. 7º).

Em relação à finalidade e ao tratamento, a Política coloca como finalidade a execução dos serviços. Em caso de aceite de coleta de dados para propósito de *marketing*, a plataforma pode "processar seu *e-mail*, número de telefone, nome e sobrenome para este fim. Você pode optar por não receber essas comunicações a qualquer momento" (Doctoralia, Política de privacidade). Quando do uso de aplicativo móvel, os dados podem ser tratados para "processar reclamações em relação aos serviços prestados; para defesa contra eles ou contra reclamações de terceiros; para informá-lo sobre novos recursos e funcionalidades de nossos serviços; e para gerenciar e planejar nossas atividades de negócios" (Doctoralia, Política de privacidade).

No caso de profissionais não cadastrados, a empresa explica que trata os dados desses profissionais para disponibilizá-los na plataforma, "a fim de informar nossos usuários de suas atividades profissionais", com vistas a permitir que os pacientes avaliem a experiência de agendamento de consulta (Doctoralia).

Em seus Termos, a plataforma inseriu uma seção denominada "Proteção de dados". Nela, assume como responsabilidade armazenar e garantir a segurança, o acesso e o uso não autorizados dos dados e das senhas dos usuários. O documento prevê os direitos de acesso, correção, edição e complementação dos dados dos usuários, incluindo os profissionais. A plataforma informa em seus Termos de uso e condições que pode incluir e editar informações sobre dados de contato do médico.

O perfil criado ou confirmado por um determinado profissional será identificado como um "Perfil verificado", possibilitando a ele: a) editar informações sobre seu perfil; b) adicionar fotos; c) responder, sob forma de comentário, às opiniões publicadas pelos usuários; d) responder perguntas feitas pelos usuários; e e) revisar as estatísticas do perfil.

Quanto aos dados de saúde, de natureza sensível, a plataforma informa em seus Termos que:

> Não faz uso de dados sensíveis de pacientes que receba, ou que sejam incluídos em seus sistemas, prontuários e demais funcionalidades, para divulgação de qualquer forma, mantendo o sigilo protegido pela legislação brasileira, salvo nos casos em que haja ordem judicial. (Doctoralia, Termos de uso)

A plataforma exige em seus Termos que as fotografias fornecidas, como contato ou durante a prestação de serviço, possam ser armazenadas, utilizadas e reproduzidas pela plataforma por meio de uma licença permanente. Esta prevê usos como:

> [...] reprodução por meios analógicos ou digitais; memória do computador; redes de informática ou multimídia; circulação pública, disponibilizar o trabalho publicamente em um local e horário selecionados pela Doctoralia; rastreio, difusão, reemissão e reprodução; arquivar a fotografia em bases de dados; e utilização da fotografia para a promoção da Doctoralia. (Doctoralia, Termos de uso)

Essa licença vai além, inclusive, do encerramento da conta. A duração do tratamento será a suficiente para os propósitos das políticas. Em geral, para a maioria das finalidades, o tempo é de cinco anos após a exclusão da conta. No caso de profissionais não cadastrados, ou daqueles cadastrados cuja finalidade é *marketing*, a guarda ocorrerá até a oposição do trabalhador da saúde.

No tocante ao compartilhamento, a plataforma exige que a aceitação dos Termos implique autorização para que os dados disponibilizados pelo profissional possam ser utilizados pela plataforma e por outros: "[...] ferramentas, aplicativos e similares, criados pela Doctoralia, ou por esta em parceria com outras empresas, para os mesmos fins a que se destina" (Doctoralia, Termos de uso). A redação é vaga para definir os mesmos "fins a que se destina". Segundo a Política, dados podem ser compartilhados com membros do grupo econômico (DocPlanner) e com provedores de terceiros para prestação de serviços ao usuário. A título exemplificativo, o documento lista quais tipos de operadores de dados podem ter acesso às informações: a) provedores de hospedagem em nuvem e manutenção de servidores; b) ferramentas de comunicação; c) ferramentas de suporte ao cliente; d) consultores externos, auditores ou conselheiros; e) prestadores de serviços de pagamento, bancos, agências de referência de crédito e prevenção de fraudes e companhias de seguros; f) empresas de TI que nos fornecem *software* e serviços similares; g) empresas que realizam a autorização de consultas e procedimentos

por meio das operadoras de plano de saúde; e h) empresas que permitem a emissão de receitas ou prescrições eletrônicas.

Também poderá haver divulgação ou compartilhamento com entes públicos para cumprimento de obrigações legais, para fazer cumprir as políticas da plataforma ou proteger os direitos e a propriedade. Os dados também serão repassados a empresas que invistam ou adquiram parcelas do conglomerado. As políticas informam que, no caso de transferência internacional, são exigidos parâmetros semelhantes aos da LGPD e do Regulamento Geral sobre a Proteção de Dados (RGPD).

As políticas elencam os direitos previstos na LGPD. O usuário pode: a) acessar o perfil do profissional de saúde (o usuário acessa as informações relacionadas a esses profissionais, a suas especialidades, seus arquivos, suas opiniões, imagens etc.); b) publicar avaliações e opiniões sobre profissionais e instituições; c) adicionar e corrigir informações sobre profissionais e instituições; d) ativar serviços de notificação de novas informações e opiniões; e) entrar em contato com os perfis de profissionais verificados; f) utilizar a ferramenta "Pergunte ao especialista" (o usuário faz perguntas e/ou consultas sobre questões médicas que serão respondidas por um dos profissionais de saúde da plataforma); g) agendar consultas *on-line* com o profissional de saúde escolhido que dispor dessa funcionalidade em seu perfil; e h) denunciar abuso.

Análise comparada e considerações conclusivas

A análise realizada no presente artigo permitiu perceber condutas distintas quanto à proteção de dados e à conformidade com a LGPD entre as plataformas analisadas, mas todas ainda distantes de uma postura mais protetiva. Nos três casos analisados, foram encontradas posturas de não garantia do básico de transparência, como detalhamentos exaustivos sobre os dados coletados, as finalidades de tratamento e as hipóteses de compartilhamento, bem como os agentes que podem ter acesso a esses dados. A ausência dessas informações indica conflito com a proteção de dados como direito constitucional e com a LGPD. Os casos avaliados são marcados por um amplo e não transparente rol de dados coletados, sempre com a possibilidade de requerimento de mais dados, por finalidades genéricas e por possibilidades muito abertas de compartilhamento.

Em geral, as empresas disponibilizam Termos de serviço e Política de privacidade, com alguns casos apenas avançando para regras específicas, como Políticas de *cookies* (Conexa Saúde). A Docway mantém regras (como Termos e Política de

privacidade) pouco claras, sem detalhamentos e com ínfima menção à legislação. Já a Conexa Saúde disponibiliza uma página voltada à informação relacionada à LGPD. A empresa fornece uma política mais detalhada, repetindo conceitos da LGPD, o que é positivo, pois não demanda que o usuário tenha que buscar a lei para ter acesso aos seus direitos e às suas obrigações.

A Doctoralia lista as bases legais para a coleta, sendo a principal delas a execução de contrato. Essa hipótese de tratamento prevista na LGPD é preocupante, pois ela substitui a base mais protetiva, a do consentimento, à qual estão ligados direitos importantes. Na prática, a adoção da base legal de execução de contrato em plataformas de trabalho tem uma implicação para a proteção de dados dos profissionais, ao reduzir os dispositivos protetivos.

A mudança dos termos ou das políticas para Política de privacidade, em geral, não é objeto de qualquer obrigatoriedade. A Doctoralia pontua em suas regras internas que não possui qualquer obrigação de comunicar novas versões a seus usuários. A Docway afirma que *poderá* (grifo nosso) comunicar as alterações nos Termos, mas assume compromisso de informar os usuários sobre ajustes na Política de privacidade. A Conexa Saúde também mantém o aviso aos trabalhadores sobre mudanças como facultativo.

Sobre a coleta de informações dos profissionais de saúde, a plataforma Docway não informa quais informações são obtidas. A Política diz apenas que serão registrados os dados fornecidos à plataforma, mas indica que poderão ser solicitados dados diversos, apresentando apenas exemplos. Há menção à coleta para uso de dados em serviços de *marketing*, mas sem discriminá-los. A Conexa Saúde apresenta um detalhamento dos dados a serem coletados dos usuários. Uma tabela detalha as bases legais, conforme a LGPD, para cada dado ou grupo de dados coletados. Contudo, esse rol não é exaustivo, uma vez que a plataforma diz poder solicitar informações adicionais e que usa *cookies*, descritos segundo suas funcionalidades, mas não quanto aos registros que obtém. A Política de *cookies* informa como recusá-los.

A empresa Doctoralia coleta diferentes grupos de dados, conforme os níveis dos perfis, com as informações listadas na Política. Assim, como nos demais casos, informa nesse documento que poderá requerer dados adicionais, mas não explicita quais são eles. A empresa ressalta que poderá coletar, inclusive, dados de dispositivos, IP, navegador e localização dos trabalhadores. O grupo utiliza *cookies*, que monitoram trabalhadores não somente para ela, mas para terceiros (como por meio dos botões de redes sociais). Mas a companhia vai além da coleta de dados dos trabalhadores, na interação da plataforma, ao reunir registros públicos

sobre eles. Assim, a Doctoralia mantém informações sobre profissionais mesmo sem eles criarem perfis na plataforma.

Chama a atenção que plataformas de saúde não tratem da coleta e do tratamento de dados sensíveis, entre os quais aqueles de saúde, em suas regras internas ou o façam de modo muito insuficiente. Apenas a Doctoralia menciona o tema, afirmando que não faz uso dessas informações "para divulgação de qualquer forma", apenas nos casos em que haja ordem judicial. O texto abre margem para compartilhamento a terceiros, desde que não haja divulgação, um risco importante. Nas demais plataformas, a ausência de uma normatização específica é ainda mais preocupante, ainda que, num dos casos (a Conexa Saúde), a coleta seja mais especificada.

Quanto às finalidades e ao tratamento, a Docway indica que as finalidades não não apresenta as finalidades de forma clara e transparente, apenas registra apontamentos genéricos que não diferenciam os tipos de usuários (pacientes ou trabalhadores) e indicam apenas propósitos gerais, como a prestação de serviços na plataforma e a "personalização da experiência do usuário". Os Termos PAD colocam uma permissão altamente ampla que na prática assegura a possibilidade de a empresa prestar quaisquer tipos de serviços. Embora o documento fale em acordo com os profissionais, isso não está explicado nem especificado, reforçando uma assimetria de poder entre a empresa e os trabalhadores. No caso das finalidades ligadas aos serviços de *marketing*, as regras da empresa também são pouco claras e não explicitam quais dados serão utilizados para quais propósitos específicos.

A Conexa Saúde elenca em sua Política de privacidade as finalidades de uso dos dados. Contudo, parte delas é bastante ampla e genérica, como "ajudar a realizar melhorias na plataforma" ou "processar dados colhidos por diferentes algoritmos internos ou de terceiros" (Conexa Saúde, Política de privacidade). Na finalidade de publicidade, o usuário precisa notificar que não deseja receber, utilizando o padrão *default*. Autores do campo destacam a importância de as configurações-padrão serem as de não coleta, ou seja, somente se o usuário autorizar os dados serão coletados. A Doctoralia também divulga finalidades de prestação de serviço. No tocante ao *marketing*, a empresa emprega a lógica de o usuário ter que optar para ter o tratamento com esse propósito.

No tocante ao compartilhamento, em geral, as plataformas apontam que poderão repassar dados a autoridades para cumprimento de obrigações legais ou para terceiros. É o caso da Conexa Saúde. Além de autoridades legais, a empresa coloca que poderá repassar informações a consultores de *marketing* e para análise

de dados, o que majora, sobremaneira, o rol de possíveis terceiros com acesso aos registros dos trabalhadores. A companhia vai além e prevê outras hipóteses de compartilhamento, mas submetidas ao consentimento do usuário. Considerando a cultura dos cidadãos de não se oporem ou não manterem suas configurações de privacidade restritas, abre-se aí outra brecha de encaminhamento abusivo dos dados dos profissionais de saúde.

A Docway afirma que não compartilha os dados com terceiros, mas apenas informações médicas com unidades de saúde e com autoridades para o cumprimento da lei. A diretriz parece conflitar com as finalidades amplas do uso dos dados, inclusive para *marketing*. Já a Doctoralia permite o compartilhamento para um rol extenso de prestadores de serviços.

A informação sobre os direitos dos titulares, especialmente os dos trabalhadores (objeto de atenção no trabalho), é elemento-chave para promover uma cultura de proteção de dados. Entre as plataformas analisadas, as abordagens foram distintas. Na Conexa Saúde, a Política de privacidade repete os direitos elencados na LGPD. Na Docway, há ínfimas menções a direitos em suas regras internas. A Doctoralia não informa o conjunto dos direitos enunciados na LGPD, mas menciona alguns deles, como o direito de o usuário se opor ao tratamento de parte dos dados e aqueles de acesso, correção, edição e complementação dos dados dos usuários.

Quanto à obrigação de disponibilizar um encarregado de proteção de dados, prevista na LGPD, a Docway não informa quem seria essa pessoa. A plataforma disponibiliza apenas um endereço de *e-mail*. Já a Conexa Saúde o faz. A Doctoralia adota conduta intermediária entre esses pontos, disponibilizando o *e-mail* institucional do Oficial de Proteção de Dados, mas sem nominá-lo.

Os casos analisados indicam ainda um longo caminho para a garantia da proteção de dados dos trabalhadores em plataformas de saúde. Apenas se considerada a ideia da proteção de dados e de sua adequação à legislação brasileira, isso em si já seria um conjunto considerável de problemas e objeto de relevantes debates jurídicos. Mas a discussão vai para além do tratamento dos profissionais de saúde de forma equivalente aos pacientes. Ao contrário, faz-se necessária uma abordagem específica que inter-relacione a proteção de dados desses profissionais com a tarefa de combater a vigilância no trabalho em plataforma, que mais além do simples acesso às informações desses indivíduos implica modelos perversos de controle das relações laborais nesses espaços.

Referências

ABILIO, Ludmila Costhek. Uberização: Do empreendedorismo para o autogerenciamento subordinado. *Psicoperspectivas*. 2019, vol.18, n.3, pp.41-51. DOI: http://dx.doi.org/10.5027/psicoperspectivas-vol18-issue3-fulltext-1674. Disponível em: http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-69242019000300041&lng=es&nrm=iso. Acesso em: 10 dez. 2023.

ALMADA, Marta, *et al*. A new paradigm in health research: FAIR data (Findable, Accessible, Interoperable, Reusable), Acta Médica Portuguesa. Ordem dos Médicos, 2020. Disponível em: http://doi.org/10.20344/amp.12910

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, v. 14, n. 3, jul.-set., p. 692-708, 2020. DOI: https://doi.org/10.29397/reciis.v14i3.2012. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2012/2391. Acesso em: 10 jan. 2024.

ASSOCIAÇÃO PAULISTA DE MEDICINA. Mercado de telemedicina na América Latina deve dobrar até 2023. **Global Telemedicine & Digital Health Summit**. 10 out. 2020. Disponível em: https://www.telemedicinesummit.com.br/artigo/mercado-de-telemedicina-na-america-latina-deve-dobrar-ate-2023/. Acesso em: 10 dez. 2023.

BALL, Kirstie, **Electronic Monitoring and Surveillance in the Workplace**. Literature review and policy recommendations. Publications Office of the European Union. Luxembourg, 2021. DOI: 10.2760/5137. Disponível em: file:///C:/Users/maria/Desktop/jrc125716_electronic_monitoring_and_surveillance_in_the_workplace_final.pdf. Acesso em: 10 dez. 2023.

BATISTA, Agnaldo de Souza. **Disseminação segura de dados pessoais vitais para apoio às tomadas de decisão em situações emergenciais**. Dissertação de Mestrado. Programa de Pós-Graduação em Informática, Setor de Ciências Exatas. Universidade Federal do Paraná. Paraná, 2019. 106 p. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://acervodigital.ufpr.br/xmlui/bitstream/handle/1884/62473/R%20-%20D%20-%20AGNALDO%20DE%20SOUZA%20BATISTA.pdf?sequence=1&isAllowed=y. Acesso em: 10 dez. 2024.

BESTSENNYY, Oleg; GILBERT, Greg; HARRIS, Alex; ROST, Jennifer. Telehealth: A quarter-trillion-dollar post-covid-19 reality? **McKinsey & Company**, 9 jul. 2021. Disponível em: https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/telehealth-a-quarter-trillion-dollar-post-covid-19-reality. Acesso em: 10 dez. 2024.

BOLAÑO, C. R. S.. Indústria Cultural, Informação e Capitalismo. São Paulo: HUCITEC, 2000.

BRASIL. Lei Nº 13.989, de 15 de abril de 2020. Dispõe sobre o uso de telemedicina durante a crise causada pelo coronavírus. Brasília, DF: Diário Oficial da União, 2000.

BRAVERMAN, Harry. **Trabajo y capital monopolista**: la degradación del trabajo en el siglo XX. México: Nuestro Tempo, 1984.

BURAWOY, Michael. **Manufacturing consent**: changes in the labor process under monopoly capitalism. Chicago: University of Chicago Press, 2012.

CAETANO, Rosangela; SILVA, Angélica Baptista; SILVA, Rondineli Mendes da; PAIVA, Carla Cardi Nepomuceno de; GUEDES, Ana Cristina Carneiro M.; RIBEIRO, Gizele da Rocha; SANTOS, Daniela Lacerda; SOUZA, Vanessa de L.; OLIVEIRA, Ione A. G. de. Educação e informação em saúde: iniciativas dos núcleos de telessaúde para o enfrentamento da covid-19. **Revista de Enfermagem do Centro-Oeste Mineiro**, v. 10, n. 1, 3888, p. 1-13, out. 2020. DOI: 10.19175/recom.v10i0.3888. Disponível em: http://seer.ufsj.edu.br/index.php/recom/article/view/3888/2522. Acesso em: 15 jan. 2024.

CAMARA, M. A. A.; LINS, G. H. A.; OLIVEIRA, F. H. C. de; CAMELO, E. M. A.; MEDEIROS, N. R. F. C. de. Internet das Coisas e *blockchain* no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados. **Cadernos Ibero-Americanos de Direito Sanitário**, v. 10, n. 1, p. 93-112, mar. 2021. DOI: https://doi.org/10.17566/ciads.v10i1.657. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/657. Acesso em: 10 fev. 2024.

CAPURRO, R.; ELDRED, M.; NAGEL D. It and privacy from an ethical perspective digital whoness: identity, privacy and freedom in the cyberworld. *In*: BUCHMANN, J. (Ed.). **Internet Privacy**: a multidisciplinary analysis. Munique: Acatech, 2012. p. 63-142.

CETIC.BR. **Pesquisa TIC Saúde 2021**. Resumo executivo. Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, 2021. Disponível em: https://cetic.br/media/docs/publicacoes/2/20211124124231/resumo_executivo_tic_saude_2021.pdf. Acesso em: 10 fev. 2024.

COLLUCCI, Cláudia. Uso de telemedicina cresce na pandemia, mas regulação enfrenta embates médicos. **Folha de S.Paulo**. 8 jul. 2021. Disponível em: https://www1.folha.uol.com.br/equilibrioesaude/2021/07/uso-de-telemedicina-cresce-na-pandemia-mas-regulacao-enfrenta-embates-medicos.shtml. Acesso em: 10 fev. 2024.

COLUSSI, Fernando Augusto Melo; SANTOS, Tomlyta Luz Velasquez dos. Novas tecnologias e liberdade de expressão na pesquisa científica: uma análise sobre a proteção de dados genéticos e de saúde. **Revista de Biodireito e Direito dos Animais**, Porto Alegre, v. 4, n. 2, p. 1- 21, jul.-dez. 2018. DOI: http://dx.doi.org/10.26668/IndexLawJournals/2525-9695/2018.v4i2.4690. Disponível em: https://www.indexlaw.org/index.php/revistarbda/article/view/4690/pdf. Acesso em: 10 fev. 2024.

CONEXA SAÚDE. **A maior plataforma independente de saúde digital**. 2024. Disponível em: https://www.conexasaude.com.br/. Acesso em: 10 fev. 2024.

CONEXA SAÚDE. **Política de privacidade**. Disponível em: https://drvirtual.s3.sa-east-1.amazonaws.com/downloads/pol_privacidade.pdf. Acesso em: 10 fev. 2024.

CONEXA SAÚDE. **Termos e condições gerais de uso, consentimento livre e esclarecido**. Disponível em: https://drvirtual.s3.sa-east-1.amazonaws.com/downloads/termo_uso_conexa_lgpd.pdf. Acesso em: 10 fev. 2024.

CONSELHO FEDERAL DE MEDICINA. **Demografia Médica no Brasil 2020**. Conselho Federal de Medicina, 2020. Disponível em: http://www.flip3d.com.br/pub/cfm/index10/?numero=23&edicao=5058#page/3. Acesso em: 10 fev. 2024.

CORDINA, Jenny; FOWKES, Jennifer; MALANI, Rupal; MEDFORD-DAVIS, Laura. Patients love telehealth – physicians are not so sure. **McKinsey & Company**, 22 fev. 2022. Disponível em: https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/patients-love-telehealth-physicians-are-not-so-sure. Acesso em: 10 fev. 2024.

DAUGAREILH, I.; DEGRYSE, C; POCHET, P. The Platform Economy and Social Law: Key Issues in Comparative Perspective. **ETUI Research Paper**, jun. 2019. DOI: http://dx.doi.org/10.2139/ssrn.3432441. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3432441. Acesso em: 20 jan. 2024.

DOCTOR.COM. **Telemedicine Adoption in the Age of covi-19 and Beyond**. Disponível em: https://www.doctor.com/resources/telemedicine?utm_source=medical_economics&utm_medium=PR&utm_campaign=telemedicine_awareness&utm_content=telemedicine_reaources#getthestudy. Acesso em: 10 jan. 2024.

DOCTORALIA. **Agende agora sua consulta**. Disponível em: https://www.doctoralia.com.br/. Acesso em: 5 set. 2023.

DOCTORALIA. **Política de privacidade e Informações sobre o tratamento dados pessoais pela Doctoralia**. Disponível em: https://www.doctoralia.com.br/privacidade. Acesso em: 15 fev. 2024.

DOCTORALIA. **Termos de uso e condições gerais para usuários e profissionais perfil básico**. Disponível em: https://www.doctoralia.com.br/termos-e-condicoes. Acesso em: 15 fev. 2024.

DOCWAY. **Docway é vencedora na categoria telemedicina**. Disponível em: https://docway.com.br/. Acesso em: 26 dez. 2023.(Docway, Termos Pronto Atendimento Digital).

DOCWAY. **Política de privacidade**. Disponível em: https://docway.com.br/politica-de-privacidade/. Acesso em: 10 dez. 2023.

DOCWAY. **Termos de uso do médico e profissional da saúde**. Disponível em: https://docway.com.br/termos-de-uso-do-medico-e-profissional-da-saude-consultorio-digital/. Acesso em: 20 dez. 2023.

DOCWAY. **Termos Pronto Atendimento Digital**. Disponível em: https://docway.com.br/. Acesso em: 20 dez. 2023.

FALEIROS JÚNIOR, J. L. de M.; CAVET, C. A.; NOGAROLI, R. Telemedicina e proteção de dados: reflexões sobre a pandemia da covid-19 e os impactos jurídicos da tecnologia aplicada à saúde. **Revista dos Tribunais**, São Paulo, v. 109, n. 1016, p 327-362, jun. 2020.

FIESELER, Christian; BUCHER, Eliane; HOFFMANN, Christian Pieter. Unfairness by design? The perceived fairness of digital labor on crowdworking platforms. **Journal of Business Ethics**, v. 156, n. 4, p. 987-1005, jun. 2019. Disponível em: https://www.jstor.org/stable/45093287. Acesso em: 20 jan. 2023.

FORTUNE BUSINESS INSIGHTS. Telemedicine market size, share & covid-19 impact analysis [...]. **Fortune Business Insights**, 2020. Disponível em: https://www.fortunebusinessinsights.com/industry-reports/telemedicine-market-101067. Acesso em: 7 fev. 2024.

WOODCOCK, Jamie; GRAHAM, Mark. The Gig Economy: A Critical Introduction. Cambridge: Polity, 2020.

HARAYAMA, Rui M. Reflexões sobre o uso do *big data* em modelos preditivos de vigilância epidemiológica no Brasil. **Cadernos Ibero-Americanos de Direito Sanitário**, v. 9, n. 3, p. 153-165, jul./set. 2020. DOI: https://doi.org/10.17566/ciads.v9i3.702. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/702. Acesso em: 15 jan. 2024.

HUWS, Ursula. Logged labour: a new paradigm of work organisation?. **Work Organisation, Labour and Globalisation**. 2016. Vol. 10(1):7-26. DOI: 10.13169/

workorgalaboglob.10.1.0007, Disponível em: https://www.scienceopen.com/hosted-document?doi=10.13169/workorgalaboglob.10.1.0007

ICICT/FIOCRUZ; INTERVOZES; IDEC. Proteção de dados pessoais em serviços da saúde digital. Resumo executivo. Rio de Janeiro. Fiocruz, out. 2022. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.icict.fiocruz.br/sites/www.icict.fiocruz.br/files/resumo_executivo_protecao_de_dados_pessoais.pdf. Acesso em: 20 jan. 2024.

KITTUR, A.; NICKERSON, J. V.; BERNSTEIN, M. S.; GERBER, E. M.; SHAW, A.; ZIMMERMAN, J. *et al.* The future of crowd work. *In*: **Proceedings of the ACM conference on computer supported cooperative work**. p. 1301-1318, 2013. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://hci.stanford.edu/publications/2013/CrowdWork/futureofcrowdwork-cscw2013.pdf. Acesso em: 5 jan. 2024.

MACEDO, Bruno Rocha de *et al.* Implantação de telemedicina de terapia intensiva durante a pandemia de covid-19. **Jornal Brasileiro de Pneumologia (JBP)**, v. 47, n. 2, p. e20200545, 2021. DOI: https://doi.org/10.36416/1806-3756/e20200545. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.br/j/jbpneu/a/bKGMwNL3CnY6SXmdkJknkBy/?format=pdf&lang=pt. Acesso em: 15 dez. 2023.

MORDOR INTELLIGENCE. Telemedicine Market & Share Analysis – Growth, Trends & Forecasts (2024 - 2029). **Mordor Intelligence**. Disponível em: https://www.mordorintelligence.com/industry-reports/global-telemedicine-market-industry. Acesso em: 15 dez. 2023.

MOROSINI, Liseane. Tecnologia a serviço da saúde: adotada em caráter emergencial na pandemia, entenda o que é telemedicina, se ela veio para ficar e como pode ajudar a ampliar o acesso à saúde. **RADIS: Comunicação e Saúde**,, fev. 2021. Disponível em: https://radis.ensp.fiocruz.br/reportagem/tecnologia-a-servico-da-saude/. Acesso em: 15 dez. 2023.

OMS (Organização Mundial da Saúde). Resolution WHA71.7. 142nd Executive Board; Genebra, 2018.

OMS (Organização Mundial da Saúde). National eHealth strategy toolkit, 2012. Disponível em: <http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH.05-2012-PDF-E.pdf>. Acesso em: 05 out. 2022.

RANI, Uma; FURRER, Marianne. Digital labour platforms and new forms of flexible work in developing countries: Algorithmic management of work and workers. **Competition & Change**, v. 25, n. 2, p. 212-236, 2021. DOI: https://doi.

org/10.1177/1024529420905187. Disponível em: https://journals.sagepub.com/doi/10.1177/1024529420905187.

RODRIGUES, G. S. N. A. *et al.* A telemedicina em tempos de covid-19 e a responsabilidade civil do médico e do hospital. *In*: CABRAL, Hildeliza Lacerda Tinoco Boechat; SILVESTRE, Gilberto F.; NETO, Ari Gonçalves. (Orgs). **As relações jurídicas e a pandemia da covid-19**. Campos dos Goytacazes: Encontrografia, 2020. p. 79-92.

ROSENBLAT, Alex; STARK, Luke. Algorithmic labor and information asymmetries: A case study of Uber's drivers. **International Journal of Communication (IJOC)**, v. 10, p. 3758-3784, 2016. Disponível em: https://ijoc.org/index.php/ijoc/article/view/4892/1739. Acesso em: 20 dez. 2023.

SAÚDE DIGITAL BRASIL – SDB. Entidade aponta que telemedicina salvou mais de 75 mil vidas entre 2020 e 2021, 2021. Disponível em: https://saudedigitalbrasil.com.br/entidade-aponta-que-telemedicina-salvou-mais-de-75-mil-vidas-entre-2020-e-2021/. Acesso em: 20 dez. 2023.

SCHMITZ, C.; HARZHEIM, E. Manual de telessaúde para Atenção Básica/Atenção Primária à Saúde. **Telessaúde Brasil Redes**, 2012. Disponível em: http://www.telessaudebrasil.org.br. Acesso em: 20 dez. 2023.

SILVEIRA, Sérgio Amadeu da. **Tudo sobre tod@ s**: redes digitais, privacidade e venda de dados pessoais. São Paulo: Edições Sesc, 2017.

VALENTE. J. Tecnologia, informação e poder: das plataformas online aos monopólios digitais. São Paulo: Ed. Dialética, 2021.

https://doi.org/10.29397/EdicoesLivres/20250104

Entre a busca de "origens" e o "planejamento da saúde": uma aproximação etnográfica dos Testes Genéticos Diretos ao Consumidor (TGDC)

Rosana Castro

"O que torna únicos os laços entre você e sua mãe?
Surpreenda-se sabendo a origem dos seus DNAs e
dezenas de predisposições
genéticas com os testes da Empresa A."
(Propaganda no site da Empresa A, maio de 2022).

A propaganda acima, publicada em data próxima ao Dias das Mães, no ano de 2022, é um dos vários exemplos de anúncios que aparecem com frequência crescente nas minhas redes sociais, ao longo dos anos de 2020 e 2022. Nesse biênio, no qual o tempo em frente às telas do computador e do celular foi amplamente exponenciado, dadas as adaptações laborais, relacionais e de entretenimento necessárias, durante a pandemia de covid-19 (Segata, 2020), surpreendeu-me notar como os testes genéticos vieram a se juntar, de forma inusitada, ao campo das tecnologias biomédicas que ganharam destaque midiático.

Se, por um lado, vacinas, medicamentos, exames diagnósticos, máscaras e outros artefatos biomédicos configuram marcas dessa pandemia, bem como discursos diversos e por vezes conflitantes sobre esses artefatos (Almeida *et al.*, 2020; Castro, 2020); por outro lado, testes genéticos como os anunciados acima, voltados à identificação de informações sobre ancestralidade e propensão ao desenvolvimento de certas doenças, entre outras finalidades, tiveram sua circulação e seu consumo significativamente ampliados nos últimos anos.

Segundo reportagem publicada no portal da revista *Veja*, em agosto de 2021, o contexto da pandemia foi particularmente oportuno para o mercado desses testes genéticos no Brasil. Empresas especializadas na venda do produto experimentaram um aumento de até 700% na demanda por seus produtos, durante os anos de 2020

e 2021 (Barros, 2021). Na mesma matéria, foi entrevistado o médico e empresário Ricardo di Lazzaro, fundador de um desses empreendimentos, que ponderou sobre possíveis razões para essa surpreendente guinada no setor: "As pessoas deixaram de viajar fisicamente e substituem essa ausência por viagens para dentro de si mesmas" (Barros, 2021). Na mesma direção, o texto da reportagem é finalizado com uma inusitada associação entre a incerteza sobre o futuro, no contexto da pandemia, e as possibilidades existenciais abertas pela realização de um teste de ancestralidade genética: "Na falta de uma resposta precisa à questão de para onde vamos, pode trazer alívio à ansiedade geral destes tempos saber que a chave para decifrar de onde viemos está na ponta de um cotonete" (Barros, 2021).

Considerando esse cenário emergente, neste ensaio, procuro fazer uma breve aproximação etnográfica pelo universo dos Testes Genéticos Diretos ao Consumidor (TGDC) no Brasil, tendo os testes de ancestralidade como ponto de partida.[13] Segundo a Sociedade Brasileira de Patologia Clínica (SBPC), com base em posicionamento e conceituação da Association for Molecular Pathology (AMP), os TGDC correspondem a "qualquer teste genético ou genômico para os quais a iniciativa de realização (*patient initiated test*) parte diretamente do consumidor, não havendo uma prescrição médica para o exame" (SBPC, *s.d.*, p. 1).

Assim, distintamente de exames clinicamente recomendados e prescritos para a composição de um diagnóstico, os TGDC configuram tecnologias nas quais a análise laboratorial do material genético está relacionada a motivações diversas de quem o consome, que podem ou não se relacionar com a saúde de modo mais direto, e prescindem de mediação ou acompanhamento médicos.

Nos casos que serão aqui descritos, parto das peças publicitárias, de *sites*, redes sociais e material jornalístico disponíveis *on-line*[14] que focalizam, inicialmente, os testes de ancestralidade e analiso como tais materiais deslizam para o anúncio de possibilidades de testagem genética para aspectos como: predisposições para desenvolvimento de diferentes doenças raras, crônicas e degenerativas; aptidões, inclinações ou resistências para certas rotinas físicas ou atividades intelectuais; preferências alimentares ou possibilidade de maior ou menor desenvolvimento de reações adversas a certos medicamentos.

Avanço, ainda, para o esforço de refletir a respeito de como são sinalizadas, por meio desse material, as possíveis vantagens do consumo dos TGDC aqui estudados para o desenvolvimento de estratégias para o "autoconhecimento" e o "planejamento

13 Utilizo aqui a tradução para o português da expressão *Direct-to-Consumer Genetic Testing*, proposta pela Sociedade Brasileira de Patologia Clínica (SBPC).

14 O material aqui analisado foi consultado entre janeiro de 2021 e maio de 2022.

da saúde", e as lógicas de subjetivação articuladas nesses processos de testagem. Assim, se por um lado, são salientadas as possibilidades de realização de um teste de ancestralidade para identificar as regiões geográficas nas quais provavelmente se encontraram os antepassados de um sujeito e ter informações sobre eventuais práticas cotidianas mais compatíveis com suas predisposições genéticas; por outro lado, nota-se como tais sugestões implicam lógicas de produção de vínculos, entretenimento e consumo que enfatizam a individualidade como eixo central de produção de "bem-estar" e "saúde".

Por fim, discuto como, em contraste com as estratégias identificadas de estímulo ao consumo dos TGDC, encontra-se um processo quase automatizado de registro do consentimento dos clientes para o compartilhamento de informações pessoais genéticas. Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), informações como as coletadas nos TGDC são classificadas como "dados pessoais sensíveis",[15] categoria que compreende dados sobre:

> [...] origem racial, 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, 2018)

Nesse sentido, reflito sobre os limites do consentimento no contexto do consumo dos TGDC para mitigação de riscos associados ao compartilhamento de dados pessoais sensíveis, sobretudo em vista das formas diversas com que os anúncios apresentam os testes – como tecnologias eficientes, não invasivas e precisas e com diferentes possibilidades de uso. Assim, nesse ambiente de consumo de produtos de empresas privadas, elaboro questões relativas à incitação ao compartilhamento de dados sensíveis, em detrimento da apresentação de informações que permitam ao cliente compreender os riscos envolvidos na contratação dos serviços e no eventual compartilhamento ou vazamento de seus dados pessoais.

Esse ensaio se organiza com o seguinte desenho: na primeira seção, farei uma breve exposição sobre a configuração do mercado nacional de TGDC, com foco em empresas que oferecem testes de ancestralidade, bem como caracterizarei os enfoques metodológico e empírico do estudo etnográfico exploratório que embasa esse trabalho.

---

15 A composição da categoria dos "dados pessoais sensíveis" é bastante semelhante à composição das "categorias especiais de dados pessoais", presente no Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia (2016) – documento que serviu de referência para a formulação da Lei Geral de Proteção de Dados Pessoais (LGPD) (Piurcosky *et al.*, 2019). No RGPD é detalhado que os dados sensíveis são assim considerados por seu processamento poder implicar "riscos significativos aos direitos e [às] liberdades fundamentais dos indivíduos" (União Europeia, 2016, p. 10).

Nas duas seções seguintes, passarei a uma discussão etnográfica das principais tendências identificadas nas publicidades investigadas nos *sites* e nas redes sociais das empresas selecionadas para essa pesquisa, com atenção para os diversos deslizamentos projetados para o consumo dos testes genéticos. Em seguida, refletirei sobre os contrastes entre as formas de comunicação das empresas, a respeito das vantagens dos TGDC, e os riscos relacionados aos modos com que o consentimento para armazenamento, tratamento e uso das informações dos clientes são coletados e registrados.

Os Testes Genéticos Diretos ao Consumidor (TGDC) no Brasil: um mercado em expansão

Os TGDC não são exatamente uma novidade no mercado brasileiro. Ao menos, desde os anos 1990, já estamos relativamente habituados com o acionamento dos testes genéticos, realizados para finalidades não diagnósticas ou não terapêuticas em diversos âmbitos da vida social. Exames de DNA para aferição de paternidade, seja em um registro jurídico, seja na espetacularização de conflitos familiares em programas de televisão, parecem ser um dos mais significativos contextos nos quais a linguagem da genética se popularizou em nosso país (Caulfield; Stern, 2017; Fonseca, 2004).

Ao lado desses testes genéticos, destacam-se, ainda, a produção e a circulação de informações, discursos, políticas acerca de exames para detecção de propensão ao desenvolvimento de doenças raras ou câncer de mama nos anos 2000, os quais articularam uma série de debates acerca de questões como parentesco, risco, consumo de tecnologias biomédicas e políticas de saúde (Aureliano, 2015; Gibbon, 2013).

Por outro lado, no início dos anos 2000, uma incandescente discussão envolvendo testes genéticos de ancestralidade ocupou diferentes veículos da mídia brasileira. Inicialmente, envolvendo o contexto da produção científica universitária, o debate teve como um de seus desdobramentos a acomodação de atividades comerciais de testes de ancestralidade no país. A divulgação dos resultados da pesquisa "Retrato Molecular do Brasil", coordenada pelo médico geneticista Sérgio Pena, da Universidade Federal de Minas Gerais, colocou em cena uma série de debates acerca da composição racial dos brasileiros (Pena *et al.*, 2000).

Nos anos seguintes, os resultados dessa pesquisa foram amplamente divulgados, mediante a divulgação de resultados de testes de ancestralidade de personalidades de diferentes áreas (pessoas dos campos artístico e esportivo) e a sua articulação teve intensa controvérsia pública sobre a legitimidade de políticas afirmativas

para negros e indígenas, nos campos da saúde e no da educação (Abel, 2020; Muniz, 2021).[16] Segundo Gaspar Neto e Santos (2011), o laboratório fundado por Sérgio Pena era o único a disponibilizar testes de ancestralidade diretamente aos consumidores no Brasil, pelo menos até o início da década de 2010.[17]

Esse cenário, no qual o mercado dos TGDC contava com uma quantidade de empresas e de consumidores bastante restrita, vem se modificando significativamente nos últimos anos. O aquecimento do campo das chamadas *healthtechs*[18] contribuiu para o impulsionamento de *startups* com produtos e serviços relacionados à análise de DNA no Brasil (Arimathea, 2021). Segundo dados divulgados no Distrito HealthTech Report (Distrito, 2020), foram investidos US$ 430 milhões em *healthtechs* no Brasil desde 2014, sendo o ano de 2017 o de maior volume de capital investido (US$ 152,3 milhões).

Por outro lado, o lançamento de testes genéticos mais baratos e com diferentes funcionalidades também concorreu para que empresas especializadas em genômica tivessem seu alcance expandido (Arimathea, 2021; Barros, 2021). Vendidos pela internet, com coleta de saliva (*swab*) feita pelo próprio consumidor, sendo o material enviado pelo correio para os laboratórios que executam as análises do DNA, tais produtos tornaram-se também, significativamente, mais baratos.[19]

O alcance dessas tecnologias, no entanto, não poderia ser justificado apenas pela expansão de investimentos no setor e pela redução de preços para acessá-las. Sua popularidade foi certamente impulsionada pelos evidentes investimentos na publicização desses produtos. Nesse contexto, as peças publicitárias ganham um destaque significativo, considerando não apenas que sua mediação estimula práticas de consumo, mas, sobretudo, pelas formas com que promovem tais práticas. Assim, nesse cenário, perspectivas antropológicas se mostram pertinentes, sobretudo na medida em que os TGDC configuram-se em artefatos que não são inertes ou anódinos – a exemplo das tecnologias biomédicas, em geral, e do material publicitário a eles associado. Ao contrário, os TGDC podem

16 Os autores do estudo "Retrato Molecular do Brasil" defendiam que os resultados de suas pesquisas apontavam para o fato de que não havia respaldo genético para atribuição de identidades raciais no Brasil, dado o alto grau de miscigenação biológica da população brasileira. Nesse sentido, desqualificavam-se as políticas afirmativas negras, ao entendê-las como "racializantes", quando biologicamente se encontrava "miscigenação" entre diferentes grupos raciais e étnicos. Movimentos negros, por outro lado, intervieram no debate público de modo a sinalizar as falácias de tal argumentação e alertar para os perigos para a luta por equidade racial no Brasil, advindos da atualização do "mito da democracia racial" em bases genéticas.

17 Sérgio Pena é também considerado um pioneiro na comercialização de testes de paternidade, exames genéticos ligados à saúde e à oferta de análises laboratoriais para investigação forense no Brasil (Zorzetto; Fioravanti, 2021).

18 De acordo com a classificação do Distrito HealthTech Report, o termo *healthtechs* designa "as soluções tecnológicas privadas no setor" de saúde (Distrito, 2020, p. 7). Segundo o mesmo relatório, a quantidade de empresas vem crescendo, significativamente, no país, sendo contabilizadas 248 *startups* brasileiras em 2018 e 542, em 2020.

19 O *kit* de coleta pode ser adquirido *on-line* e recebido em casa, contando com o material necessário para a coleta do DNA e as instruções sobre como fazê-la. O *kit* é, então, enviado para análise. E o cliente tem os resultados dos exames, após algumas semanas, por meio de acesso a uma área no *site* da empresa, com uso de *login* e senha pessoais. O kit de algumas marcas pode ser também encontrado em drogarias.

ser abordados como objetos técnicos, que somente são compreensíveis, quando levados em conta as suas articulações materiais e políticas. De acordo com a socióloga Madeleine Akrich (2014):

> Os objetos técnicos definem, em sua configuração, uma certa partição do mundo físico e social, atribuem certos papéis a certos tipos de atores – humanos e não humanos – excluindo outros, autorizam certos modos de relação entre estes diferentes atores etc. [...] de maneira tal que eles participam plenamente da construção de uma cultura, no sentido antropológico do termo, ao mesmo tempo em que eles se tornam obrigatoriamente os mediadores em todas as relações que nós mantemos com o "real". (Akrich, 2014, p. 161)

A compreensão da ação das peças publicitárias é fundamental no esforço de análise dos modos com que os TGDC têm construído suas legitimidades – seja como técnica confiável para produção de informações, seja como produto de consumo que se articula criativamente a uma malha complexa de usos e significados socioculturais (Azize, 2006).

Neste trabalho, parto dos testes de ancestralidade para salientar os principais elementos por meio dos quais as propagandas de TGDC agenciam estratégias para sustentar a pertinência e as vantagens do produto, ao mesmo tempo em que acionam essa modalidade de testagem como chamariz para a venda de análises com resultados, potencialmente, incorporados aos usos voltados à "saúde" e ao "bem-estar".

No contexto da pandemia de covid-19, o impulsionamento de propagandas direcionadas para potenciais consumidores pelos algoritmos parece ter funcionado como uma estratégia importante de popularização dos testes de ancestralidade e de propulsão para as suas vendas. O resultado de tamanho investimento não é de se ignorar. Segundo reportagem publicada no *Estadão*, em fevereiro de 2021: "[...] no Brasil, a pesquisa por esses exames no Google viu um crescimento de até 300% nos últimos 12 meses, o que indica espaço para crescimento do mercado" (Arimathea, 2021).

A aproximação etnográfica ora proposta tem seu foco sobre ações e peças publicitárias de duas das principais empresas do mercado brasileiro.[20] A primeira

20 No campo mais amplo dos TGDC, há várias empresas focadas em testes genéticos, no campo da saúde, abrangendo desde exames em embriões humanos até análises post mortem, alcançando ainda outras que investem, por exemplo, em exames genéticos para fins de aprimoramento de performances esportivas.

delas é a Empresa A, fundada na década de 2010. O laboratório trabalhou com diferentes exames genéticos por aproximadamente dez anos, quando passou a focar seus negócios na venda de testes genéticos de "ancestralidade", "saúde" e "bem-estar". Aparentemente, essa estratégia inaugurou um momento de grande sucesso da empresa, tendo sido registrado em matérias jornalísticas que o negócio experimentou grande crescimento no ano de 2020 e multiplicou, significativamente, suas vendas em 2021.

A segunda empresa, cujo material publicitário será aqui analisado é a Empresa Z, fundada também na década de 2010. A empresa faz parte de um conjunto de empreendimentos com farta experiência na realização de exames genéticos para aplicação clínica, e tem tido seu alcance ampliado nos últimos anos, a partir do lançamento de *kits* domésticos de testes de ancestralidade e de exames para avaliação de predisposições ao desenvolvimento de algumas doenças hereditárias.

Nas duas próximas seções, procuro sinalizar algumas linhas de força dos modos de caracterização dos TGDC em peças e ações publicitárias dessas empresas. Nesse processo, saliento os principais enquadramentos produzidos para o consumo desses produtos, bem como os modos de subjetivação construídos e projetados no anúncio dessas tecnologias.

Buscando o passado: autoconhecimento, entretenimento e consumo

> Se um dia te perguntassem o que você tem para se dizer, será que você conseguiria dizer quais são as suas origens? O seu passado? Por onde seus ancestrais passaram? Saberia olhar para dentro de você e dizer qual a relação do seu DNA com o seu futuro? Saberia? Você pode não saber nenhuma dessas coisas, mas, acredite, o seu DNA sabe. (Vídeo comercial do teste de ancestralidade da Empresa A, 2021)

O texto acima foi interpretado por um artista brasileiro negro, compondo o áudio do comercial da empresa, disponível em seu *site* e em seu canal no YouTube. Embora a voz que emite todas essas palavras seja a do artista, nas imagens do comercial, o texto é mimetizado por outros atores e atrizes de diferentes identificações étnico-raciais, tendo ao fundo uma música com sons de tambores, guitarras e efeitos eletrônicos. Seus corpos estão pintados com linhas tortuosas brancas e sobre eles são projetadas luzes diversas, enquanto, ao fundo da imagem, paisagens sortidas se entrelaçam com os sons do texto e da canção – tudo parece compor uma

espécie de mosaico vivo. Ao final do vídeo, a imagem do protagonista é ladeada pelos resultados de seu teste de ancestralidade e por um mapa animado das regiões mencionadas a cada novo resultado lançado na imagem, com percentuais atribuídos a parcelas de sua ancestralidade. Há menções às regiões dos continentes africano e europeu, bem como a um grupo indígena americano. O vídeo é, então, finalizado com a marca da empresa, junto da frase: "busque em você".

Com mais de 8 milhões de visualizações até maio de 2022, esse vídeo sintetiza uma série de motes técnicos e simbólico-políticos do teste de ancestralidade da empresa. Segundo Abel (2020, p. 189), os testes de ancestralidade genética são "uma técnica que usa o genoma como uma lente para adentrar nossa ancestralidade biológica, expressando-a em relação a populações geograficamente definidas". O apelo para o consumo dos testes de ancestralidade, assim, articula-se por meio da apresentação de suas potencialidades de produção de "autoconhecimento", a partir da identificação de regiões geográficas, nos quais antepassados do consumidor teriam habitado ou transitado, e da transposição dessas informações de volta ao presente.

Ao configurar e performatizar o corpo (Mol, 2002) de usuários da tecnologia como uma espécie de arquivo (Abel, 2020), e, mais precisamente, configurando a materialidade do DNA como um artefato-fonte de conhecimento, o teste de ancestralidade emerge como um mediador fundamental entre o presente e o passado, um passaporte para dimensões espaço-temporais profundas de um indivíduo.[21]

Nesse complexo fluxo temporal, as possibilidades de uso de informações genéticas não ficam restritas a uma dimensão arquivística, mas se desdobram na sugestão de sua pertinência em diferentes contextos cotidianos. No *site* da Empresa Z, por exemplo, os testes de ancestralidade são sumariamente descritos como exames que revelam não somente a ancestralidade genética, mas informações históricas e sociais sobre os povos de origem genética do consumidor. Ao enfatizar as informações adicionais disponibilizadas nos perfis dos clientes, a partir dos resultados numéricos de seus testes, a empresa descreve, ainda, que não se trata apenas de um exame, na medida em que seus resultados permitem que o cliente não só conheça sua ancestralidade, mas estabeleça conexões com ela.

Tais experiências de "conexão" se configuram a partir do material adicional que acompanha os resultados dos testes de DNA. Os dados numéricos, que conformam o resultado do teste de ancestralidade, se desdobram em informações acerca de

21 Há mais uma dimensão significativa da busca do passado articulada ao uso do material genético, relacionada à procura de parentes, com o pareamento das informações genéticas em uma plataforma específica – modalidade que costuma ser publicizada, a partir de casos de consumidores que foram adotados e que procuram encontrar familiares desconhecidos ou com os quais perderam contato. Dadas as limitações deste ensaio e o momento ainda inicial desta investigação, não me debruçarei sobre as especificidades desse tipo de testagem.

tradições, costumes e expressões culturais de populações das regiões geográficas correspondentes à ancestralidade de cada cliente. Esses resultados sugerem um estímulo para que o percurso trifásico, previsto na aquisição do exame, se complete: fazer o teste, conhecer sua ancestralidade, conectar-se com ela. Para tanto, a marca oferece recomendações de elementos como filmes, restaurantes, receitas, músicas e outros artefatos, sugerindo que os resultados de exames possibilitam que os clientes se enxerguem como parte dos grupos representados nos números e nos materiais adicionais que acompanham os resultados dos testes de ancestralidade.

Informações adicionais ao perfil numérico de ancestralidade são oferecidas também pela empresa A. Na amostra dos resultados disponibilizada pela empresa em seu *site*, a ancestralidade de um indivíduo é apresentada nos moldes da representação descrita no início desta seção, porém com diferentes percentuais e regiões representados. Para cada uma das regiões geográficas descritas, há um detalhamento de sub-regiões, países ou grupos étnicos que contribuíram com percentuais específicos para a ancestralidade do sujeito. Por sua vez, para cada um desses locais, há um pequeno texto no qual constam informações histórico-geográficas sobre a região e os povos que nela viveram, vivem ou passaram.

A disposição dessas informações, por sua vez, aponta para possibilidades diversas de consumo dos exames, deslizando as finalidades associadas ao "autoconhecimento" para as atividades de entretenimento[22] e para o fomento do consumo –, para além do usuário inicial ou do próprio teste de ancestralidade. Assim, no *site* da empresa Z, esses testes são descritos como uma tecnologia, cujo uso seria vantajoso, pois associava a ancestralidade genética à identidade pessoal de um indivíduo. Já as informações adicionais oferecidas pela empresa A podem ser direcionadas, por exemplo, para a aquisição de pacotes de passeios e viagens relacionados aos resultados dos exames. Nesse cenário, os testes de ancestralidade assumem uma feição adicional relacionada ao entretenimento e ao lazer vinculados ao consumo, no qual as informações genéticas proporcionam uma série de outras atividades, nas quais o "autoconhecimento" pode ser implicado.

Nesse caminho, os testes de ancestralidade são, ainda, promovidos como tecnologias que ensejam sociabilidade, são também anunciados como possibilidades de presentes criativos a serem distribuídos em diferentes ocasiões. Anunciado no *site* da empresa Z como um presente inusitado ou

22 Bolnick et al. (2007) utilizam a categoria "recreacional" para tratar amplamente de testes genéticos de ancestralidade, fazendo referência à categorização, então, corrente nos Estados Unidos que, acredito, assemelha-se ao tensionamento acionado no contraste entre usos "terapêuticos" e "recreativos" de substâncias farmacêuticas. Como apresentado adiante, essa categoria também figura na classificação da SBPC.

mesmo surpreendente, o teste de ancestralidade é sugerido como uma forma de oferecer a terceiros a possibilidade de se viver diversas experiências na busca pela ancestralidade. Chamam atenção, nesse mesmo sentido, as campanhas promocionais para diferentes momentos do calendário – desde os Dias das Mães e dos Pais, passando pelo Dia dos Namorados, até descontos especiais nos dias circunvizinhos à Black Friday.

O apelo publicitário dos testes de ancestralidade aponta para diferentes direções, nas quais são combinadas sugestões de viagens ao interior, na busca por "autoconhecimento", e, ao exterior, para se ir ao encontro das raízes de sua ancestralidade, em uma dinâmica que implica deslizamentos e desdobramentos entre o resgate de informações referentes à identidade dos sujeitos e as possibilidades de troca de presentes. Tais dimensões adensam momentos anteriores, nos quais os testes de ancestralidade, vendidos diretamente aos consumidores, tinham disponibilidade, circulação e possibilidade de acesso financeiro mais restritos (Gaspar Neto; Santos, 2011).

Por outro lado, as análises de DNA, voltadas para usos de saúde, mais amplamente difundidas no cenário nacional, não estão ausentes desse universo aqui investigado. Pelo contrário, na análise preliminar aqui apresentada, os testes de ancestralidade funcionam como um chamariz para potenciais consumidores de outros exames que, adquiridos como serviços adicionais, compõem o universo mais amplo dos TGDC. Na próxima seção, tratarei de alguns desses deslizamentos.

Administrando o futuro: predisposições e escolhas no "planejamento da saúde"

"Planeje seu 2022 através do seu DNA". Esta frase estampava um anúncio na página inicial do *site* da empresa A, no final do ano de 2021, ao lado da imagem de dois jovens, um homem e uma mulher brancos, que estavam em segundo plano. No primeiro plano, faíscas de uma vela e, no terceiro, imagens de fogos de artifício estourando, dividiam espaço com a imagem do *kit* de testagem da marca. O *banner* eletrônico era composto pela frase – "Entenda mais sobre você e sobre seu futuro a partir de sua genética" –, seguida de uma palavra que, digitada no momento da compra no *site*, permitiria ao cliente adquirir os produtos da empresa com um desconto de 22% – em referência ao ano que se iniciaria em poucos dias. Tratava-se de uma promoção de *Réveillon*, e o mote principal do anúncio eram as possibilidades de uso dos resultados dos exames de DNA relacionados à saúde para os planos e os projetos do ano-novo.

Os produtos anunciados eram dois pacotes de testagem genética da empresa A, voltados ao "bem-estar" e à "saúde". O primeiro teste trazia resultados de análises de DNA relacionadas às questões do "corpo" e da "mente", enquanto o segundo fornecia dados sobre os modos com que os resultados do teste genético se relacionavam com os efeitos de certos medicamentos e com o potencial de desenvolvimento de certas doenças. De modo mais abrangente, os exames podem ser descritos como aqueles que determinam correlações entre as informações genéticas e a absorção de certas substâncias alimentares e farmacêuticas; indicam os melhores hábitos de exercícios físicos; apresentam questões de envelhecimento; e trazem os traços de personalidade. Os resultados são amplos e variados, sobrepondo, por exemplo, informações sobre chances de desenvolvimento de doenças, como diabetes, e condições como tremores e calvície, análises sobre dietas que seriam mais adequadas a um certo perfil genético, predisposições a maior ou menor resistência muscular e *performance* esportiva e tendências comportamentais específicas em contextos de estresse.

Essa linha de produtos enfatiza, ainda, uma aproximação entre as predisposições genéticas e o desenvolvimento de hábitos e preferências ou a dificuldade de manutenção de certas rotinas. Nas redes sociais da empresa, chamam atenção, por exemplo, postagens que procuram sinalizar possibilidades de recomendação das melhores modalidades de exercício físico para cada indivíduo, com base no resultado de exame de DNA e com vistas à otimização dos resultados. Na mesma direção, uma outra postagem promocional do Dia do Amigo era formada pela fotografia de duas jovens abraçadas, uma branca e outra negra, acompanhada de uma pergunta sobre qual tipo de amizade seria mais compatível com o potencial consumidor, com base no DNA. Na imagem seguinte, resultados de testes genéticos dessa linha eram associados a tópicos que, por sua vez, corresponderiam a certos perfis de personalidade e amizade. Os outros exames dessa linha de produtos recomendavam que, a partir dos resultados dos testes, usuários deviam fazer alterações e adaptações em suas rotinas alimentares, de exercícios físicos e cuidados com o corpo, personalizando-as, segundo necessidades e inclinações específicas identificadas nos testes.

Na mesma direção, uma linha específica de testes da empresa Z foca seus resultados em exames genéticos para detecção de genes relacionados a questões como o desenvolvimento de alguns tipos de câncer, os níveis elevados de colesterol e triglicerídeos e as doenças genéticas raras. No *site* da marca, a realização desses testes é estimulada pela associação do consumo do teste com o cuidado do potencial consumidor com "o seu futuro", projetando-se, assim, a

perspectiva de uso das análises genéticas para a tomada de decisões relativas ao curso da vida.

Nesse contexto, o exame de DNA é articulado como um artefato que, simultaneamente, aciona uma conduta individual precavida, na qual a não identificação de predisposição para o desenvolvimento de uma das doenças implica o sujeito em uma postura de cuidado antecipado – e possível despreocupação futura. Ou, em caso de identificação de algum marcador genético associado a essas condições, compreende-se a possibilidade de ele procurar um profissional para verificar se tal situação está instalada ou, em caso negativo, realizar um acompanhamento.

Em uma postagem da empresa Z, nas redes sociais, por exemplo, explica-se em um *card* que os testes genéticos dessa linha identificam doenças genéticas antes mesmo de aparecerem sintomas a elas associadas, possibilitando que consumidores antecipem eventuais cuidados e intervenções médicas. Nessa mesma direção, nessa rede social, um vídeo protagonizado por uma celebridade se destaca, não somente pelo acionamento de uma personalidade para um anúncio, mas pelo modo com que ela, ao retomar sua experiência de cura de um câncer, conclama os seguidores a assumirem uma postura ativa com relação à sua saúde, adquirindo um teste de DNA:

> Durante o tratamento, eu descobri que um em cada dez casos de câncer [...] é hereditário. Isso quer dizer que ele surge por causa de alterações que podem estar no seu DNA, no DNA da nossa família. Mas essas alterações genéticas que aumentam também a predisposição a outros tipos de câncer podem ser identificadas com antecedência, através de testes genéticos como este.

Os testes genéticos para identificação de aspectos relacionados ao "bem-estar" e à "saúde" configuram uma linha importante de atuação das duas empresas aqui estudadas –, embora os testes de ancestralidade pareçam ter um destaque maior nas estratégias de divulgação de produtos em *sites* e redes sociais. As ênfases em aspectos específicos da saúde, da personalidade e do estilo de vida relacionados ao DNA e as predisposições a ele associadas implicam projeções de um público de consumidores preocupados com o futuro e dispostos a planejar suas condutas e seus hábitos, a partir das informações produzidas pelos testes genéticos.

Assim, mesmo que os testes possam levar a uma consulta médica, a iniciativa de busca e produção de informações é feita pelo indivíduo que se propõe a comprar

um teste genético – e tem condições de fazê-lo – e a assumir uma postura de administração de sua saúde. Em uma reportagem publicada pelo *Estadão*, um usuário de teste genético desse tipo reforçou essa perspectiva. Ao dar seu depoimento, o homem de 36 anos destacou que:

> Eu não tinha costume de fazer exames de saúde e fiz o teste biológico, que apontou que eu tinha propensão elevada para algumas doenças. Há duas semanas, eu fiz um *check-up* e os resultados revelaram que eu já estou apresentando essas doenças. Foi bastante útil para planejar minha saúde, apesar de os dados no Brasil ainda serem limitados. (Arimathea, 2021)

Consumo de testes genéticos e compartilhamento de dados sensíveis: reflexões preliminares

A testagem genética, conforme procurei descrever, articula-se em um complexo agenciamento entre os elementos do *kit* de coleta, a análise do DNA, a interação com diferentes informações disponibilizadas no *site* e as possibilidades de diferentes disposições subjetivas do cliente quanto a si mesmo, à sua história e ao seu futuro.

Apesar das diferenças temporais vetoriais entre as peças publicitárias e os *sites* nos quais figuram ambos os tipos de teste, tais tecnologias procuram sinalizar diversos usos e articulações cotidianas das informações prestadas nos resultados dos exames. Desde as possibilidades de responder perguntas prosaicas sobre o conhecimento de suas "origens" até tomadas de decisão baseadas em um percentual de chance de desenvolvimento de um câncer, passando pela possibilidade de estender tais atividades para viagens, passeios e interações com pessoas com ancestralidade e predisposições genéticas comuns. A multiplicidade e a sobreposição dessas possibilidades de articulação embaralham classificações estanques.

A SBPC classifica os TGDC nas seguintes categorias: I) clinicamente úteis: oferecem informações significativas para a realização de diagnóstico, predição, prognóstico ou acompanhamento terapêutico; II) interesse comercial: não têm aplicação clínica e se associam à venda de produtos ou serviços de uma certa empresa; III) ancestralidade: oferecem informações sobre vínculos biológicos entre indivíduos e grupos; IV) recreacionais: produzem informações genéticas que atendem à "curiosidade" dos interessados (SBPC, *s.d.*).

Ao se observar o material publicitário aqui analisado, é notável como o encaixe dos testes em apenas uma dessas categorias seria precário, dadas as possibilidades sobrepostas de motivações de uso presentes nos anúncios. Mais que isso, o extensivo potencial de uso presente nas propagandas se articula ao engendramento de um certo *script* (Akrich, 2014), no qual o usuário individual é pronunciadamente articulado como sujeito responsável por sua saúde e seu bem-estar, seja no presente, seja no futuro.

Nesse sentido, destaco como a investigação de predisposições genéticas, recebidas hereditariamente, são engendradas numa linguagem de risco que, por sua vez, projeta sobre o consumidor um conjunto de responsabilidades (Aureliano, 2015). Nesse caso particular, trata-se de ativamente "planejar sua saúde", investindo em conhecimentos moleculares sobre seu corpo e exercendo escolhas sobre o presente, de modo a administrar o futuro.

Esse modo de subjetivação apresenta continuidades com um conjunto de práticas já investigadas nos campos da antropologia e da saúde coletiva, nos quais um indivíduo autocentrado e empreendedor de si investe em seu corpo ao se engajar em uma série de atividades relacionadas à sua saúde e ao seu bem-estar, mediadas pelo consumo de tecnologias biomédicas (Azize, 2006; Rohden, 2017). No entanto, se esses estudos salientam como lógicas de gerenciamento individual e aprimoramento se associam e sobrepõem ao uso de medicamentos, substâncias e outras formas de intervenção corporal, aqui encontramos indícios do avanço de tendências que centram sobre os indivíduos e as suas escolhas a descoberta das explicações sobre si e para si e o manejo dessas informações no modelamento de sua trajetória, sua história e sua saúde.

O reforço de lógicas individualizantes articuladas no material publicitário contrasta, de modo significativo, com aspectos relacionados ao pressuposto fundamental para a produção de informações por meio dos TGDC: o compartilhamento de dados pessoais com as empresas fabricantes. Enquanto os testes genéticos são vendidos como soluções fáceis e rápidas, podendo o procedimento de coleta de saliva ser realizado pelo próprio consumidor, dimensões econômicas, éticas e políticas, relacionadas ao armazenamento, ao tratamento, ao processamento e ao eventual compartilhamento desses dados coletados no processo de compra, na análise do material biológico e na entrega dos resultados *on-line*, essas outras dimensões não ganham o mesmo destaque dos anúncios.

Por um lado, diferentemente de informações acerca das funcionalidades dos testes apresentadas nos *sites* e nas redes sociais, por meio de fartas e diversificadas estratégias de comunicação, os termos e as políticas de

privacidade das marcas são disponibilizados em *links* posicionados nas partes mais inferiores da página inicial dos *sites* e seu conteúdo acessível apenas, indiretamente, a partir dos perfis das marcas em redes sociais. Cabe mencionar, em todo caso, que as políticas das duas empresas estudadas sinalizam adequação à LGPD (Brasil, 2018).

Por outro lado, o consentimento dos consumidores, no momento da compra via *site*, relativo à sua privacidade e ao compartilhamento de dados – sejam as informações genéticas propriamente ditas, sejam os dados coletados nos procedimentos de cadastro e na navegação do *site* –, é realizado em um sistema do tipo *clickwrap*. Isso se dá por meio de um clique numa caixa, cujo texto consiste numa afirmação em primeira pessoa, na qual o cliente declara que leu e concordou com as políticas, os termos e as condições da empresa – que incluem, mas não se restringem às questões relativas à proteção de dados pessoais – e consente quase que automaticamente com uma série de procedimentos dos quais não é necessário sequer tomar conhecimento. Essa caixa precede o clique que concretiza a compra do teste e a contratação das análises laboratoriais, situação na qual, por um lado, fica mais visível o *link* de acesso às políticas de privacidade e, por outro, pouco se instrui ativamente o cliente para que ele possa conhecer eventuais riscos relativos ao envio de material genético para empresas privadas, no contexto da contratação desses serviços.

Assim, o "autoconhecimento", o entretenimento e a administração da "saúde" e do "bem-estar", por meio da compra de testes genéticos, são largamente enfatizados, enquanto os riscos relacionados ao compartilhamento de dados são secundarizados e rapidamente devolvidos aos clientes, já que eles consentem com os procedimentos e os riscos do uso da tecnologia. Entre esses riscos estão as possibilidades de compartilhamento futuro de dados entre empresas, entre setores do Estado, e o vazamento de informações – a depender do modo como essas informações forem apropriadas, elas podem fragilizar o titular. Seria o caso, por exemplo, de uso de um determinado resultado de exame genético, que identifica predisposição a uma certa doença, para aumentar o valor de um título de plano de saúde, ou recusar o acesso de certo sujeito a algum serviço público.

Por fim, nota-se uma eloquente ausência de informações sobre a composição de bancos de dados, a partir do material genético dos clientes, as eventuais formas de uso e o compartilhamento e o potencial financeiro. No estudo exploratório dos documentos, nas páginas e postagens das empresas aqui citadas, em diversos momentos, comenta-se que os dados genéticos individuais são cotejados com bancos de dados mais amplos, de modo a realizar comparações. Por outro lado,

não foram encontradas informações detalhadas a respeito da possibilidade de os dados dos clientes formarem um banco de dados que servirá de base para comparações com testes de outros indivíduos, inclusive por mediação de outras empresas ou instituições públicas.

Não é de se ignorar o potencial financeiro dessas informações, as quais, tomadas em conjunto, já configuram um importante ativo comercial e um alvo de interesse de grupos de atividade ilícita no universo digital (Regalado, 2016; Roncolato, 2018). Assim, é legítimo ponderar "se" e "de que maneira" a expansão do consumo de TGDC e a especulação comercial, que acompanham essa atividade, podem implicar usos e compartilhamentos de dados distintos daqueles previstos no momento da compra.

Comentários finais

Desde o início da pandemia de covid-19, o desenvolvimento de diferentes tecnologias que permitissem mitigar ou contornar os efeitos deletérios do contágio pelo vírus SARS-CoV-2 imprimiu uma acelerada corrida tecnológica em laboratórios e universidades ao redor do mundo. Nesse contexto, no qual o recurso às tecnologias biomédicas foi intensificado, a circulação e o consumo de TGDC tiveram um inusitado destaque. Anunciados em perfis de redes sociais e em outras plataformas da internet por artistas de renome, além de jornalistas, atletas e influenciadores digitais, os TGDC têm tido sua popularidade bastante aumentada nos últimos anos. Os testes de ancestralidade, foco inicial deste estudo, destacam-se por se estabelecerem como produto carro-chefe de empresas de recente propulsão no mercado nacional, sendo ele uma espécie de porta de entrada de consumidores "curiosos", no universo dos exames voltados a dimensões adicionais, como "saúde" e "bem-estar".

A expansão rápida e exponencial no consumo dos TGDC no Brasil coloca uma série de dilemas e questões quanto às possibilidades e aos limites da LGPD de garantir a proteção de dados genéticos nesse contexto altamente dinâmico e competitivo. No contexto da proteção de dados, o consentimento individual é o principal fator por meio do qual essa lei visa garantir que direitos e liberdades não sejam violados. Ocorre que os modos de consentimento automatizado, na aquisição de testes genéticos, parecem garantir mais que as empresas estejam juridicamente seguras, ou seja, que não sofrerão eventuais punições, e menos que os clientes tenham seus direitos preservados, enquanto as empresas tiverem acesso aos seus dados genéticos.

Diante de iniciativas publicitárias diversificadas e de tamanho alcance, cabe considerar diferentes dimensões relativas ao consentimento prestado, durante o consumo, bem como colocá-lo em perspectiva diante das estratégias e dos apelos de convencimento apresentados aos potenciais consumidores. Nesse contexto, no qual empresas concentram poder na governança de dados pessoais sensíveis, o debate e o fomento de iniciativas coletivas protagonizadas por grupos da sociedade civil para regulamentação do manejo de tais informações são urgentes e indispensáveis.

Referências

ABEL, Sarah. Rethinking the "Prejudice of Mark": Concepts of Race, Ancestry, and Genetics among Brazilian DNA Test-Takers. **Odeere: Revista do Programa de Pós-graduação em Relações Étnicas e Contemporaneidade (PPGREC)**, v. 5, n. 10, p. 186-221, jul.-dez. 2020. DOI: 10.22481/odeere.v5i10.7181. Disponível em: file:///C:/Users/maria/Desktop/7181-Texto%20do%20artigo-16380-3-10-20210104.pdf. Acesso em: 20 dez. 2023.

AKRICH, Madeleine. Como descrever os objetos técnicos? **Boletim Campineiro de Geografia: Revista Científica da Associação dos Geógrafos Brasileiros Seção Campinas**, v. 4, n. 1, p. 161-182, 2014. DOI: https://doi.org/10.54446/bcg.v4i1.147. Disponível em: https://publicacoes.agb.org.br/boletim-campineiro/article/view/2516. Acesso em: 7 jan. 2024.

ALMEIDA, Bethania de Araujo *et al.* Preservação da privacidade no enfrentamento da covid-19: dados pessoais e a pandemia global. **Ciência & Saúde Coletiva: Revista da Associação Brasileira de Saúde Coletiva**, v. 25, n. 6, supl., p. 2487-2492, jun. 2020. Disponível em: https://cienciaesaudecoletiva.com.br/artigos/preservacao-da-privacidade-no-enfrentamento-da-covid19-dados-pessoais-e-a-pandemia-global/17570?id=17570. Acesso em: 10 fev. 2024.

ARIMATHEA, Bruna. Testes de DNA ficam mais acessíveis no Brasil com presença de *startups*. **Estadão**, 28 fev. 2021. Disponível em: https://link.estadao.com.br/noticias/empresas,testes-de-dna-ficam-mais-acessiveis-no-brasil-com-presenca-de-startups,70003629684. Acesso em: 15 maio 2022.

AURELIANO, Waleska de A. Health and the Value of Inheritance: The meanings surrounding a rare genetic disease. **Vibrant: Virtual Brazilian Anthropology**, v. 12, n. 1, p. 109-140, 2015. DOI: https://doi.org/10.1590/1809-43412015v12n1p109. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.br/j/vb/a/4QbPFMBYXgW795yMKLcbg7x/?format=pdf&lang=em. Acesso em: 3 jan. 2024.

AZIZE, Rogério Lopes. Saúde e estilo de vida: divulgação de medicamentos em classes médias urbanas. *In*: LEITÃO, D. K.; LIMA, D. N. de O.; PINHEIRO-MACHADO, R. (Orgs.). **Antropologia e consumo**: diálogos entre Brasil e Argentina. Porto Alegre: AGE, 2006. p. 119-137.

BARROS, Duda Monteiro de. Testes genéticos que mapeiam origem dos ancestrais estão em alta no Brasil. **Veja**. 6 ago. 2021. Disponível em: https://veja.abril.com.br/ciencia/testes-geneticos-que-mapeiam-origem-dos-ancestrais-estao-em-alta-no-brasil. Acesso em: 12 fev. 2024.

BOLNICK, Deborah A. *et al.* The Science and Business of Genetic Ancestry Testing. **Science**, v. 318, n. 5849, p. 399-400, out. 2007. DOI: 10.1126/science.1150098. Disponível em: https://www.science.org/doi/10.1126/science.1150098. Acesso em: 10 jan. 2024.

BRASIL, Presidência da República. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 fev. 2022.

CASTRO, Rosana. Ciências e tecnologias na pandemia de covid-19: exposições, experimentos, expectativas. GROSSI, M. P.; TONIOL, R. (Orgs.). **Cientistas sociais e o coronavírus**. São Paulo: ANPOCS; Florianópolis: Tribo da Ilha, 2020. p. 359-362.

CAULFIELD, Sueann; STERN, Alexandra Minna. Shadows of doubt: the uneasy incorporation of identification science into legal determination of paternity in Brazil. **Cadernos de Saúde Pública**, v. 33, n. 13, supl. 1, p. e00110016, 2017. DOI: 10.1590/0102-311x00110016. Disponível em: https://cadernos.ensp.fiocruz.br/ojs/index.php/csp/article/view/6465. Acesso em: 15 dez. 2023.

DISTRITO. **HealthTech Report 2020**. *s.l.*: Distrito, 2020. Disponível em: https://materiais.distrito.me/mr/healthtech-report#hs_cos_wrapper_widget_1620060789692_. Acesso em: 15 maio 2022.

FONSECA, Claudia. A certeza que pariu a dúvida: paternidade e DNA. **Revista Estudos Feministas**, v. 12, n. 2, p. 13-34, ago. 2004. DOI: https://doi.org/10.1590/S0104-026X2004000200002. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.br/j/ref/a/7BqFfPVPj5QjLfbVytx8DgQ/?format=pdf&lang=pt. Acesso em: 10 jan. 2024.

GASPAR NETO, Verlan Valle; SANTOS, Ricardo V. Biorrevelações: testes de ancestralidade genética em perspectiva antropológica comparada. **Horizontes Antropológicos**, v. 17, n. 35, p. 227-255, jan.-jun. 2011. DOI: https://doi.org/10.1590/S0104-71832011000100008. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.br/j/ha/a/tSWw9FqWC7wPHjvw4qSzpRt/?format=pdf&lang=pt. Acesso em: 10 jan. 2024.

GIBBON, Sahra. Ancestry, Temporality, and Potentiality: Engaging Cancer Genetics in Southern Brazil. **Current Anthropology**, v. 54, n. 57, p. S107-S117, 2013. DOI: https://doi.org/10.1086/671400. Disponível em: https://www.journals.uchicago.edu/doi/full/10.1086/671400. Acesso em: 15 fev. 2024.

MOL, Annemarie. **The body multiple**: Ontology in Medical Practice. Durham: Duke University Press, 2002.

MUNIZ, Tatiane P. **Processos de materialização da raça e do racismo no campo da saúde**: uma etnografia das práticas e narrativas profissionais. Tese de Doutorado. Programa de Pós-Graduação em Antropologia Social. Universidade Federal do Rio Grande do Sul, Porto Alegre, 2021. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://lume.ufrgs.br/bitstream/handle/10183/229816/001131046.pdf?sequence=1&isAllowed=y. Acesso em: 15 fev. 2024.

PENA, Sérgio D. J. *et al.* Retrato molecular do Brasil. **Ciência Hoje**, v. 27, n. 159, p. 16-25, abr. 2000. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://labs.icb.ufmg.br/lbem/pdf/retrato.pdf. Acesso em: 10 jan. 2024.

PIURCOSKY, Fabrício Pelloso *et al.* A Lei Geral de Proteção de Dados Pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma de Negocios**, v. 10, n. 23, p. 89-99, jul.-dez. 2019. DOI: http://dx.doi.org/10.14349/sumneg/2019.V10.N23.A2. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://blogs.konradlorenz.edu.co/files/rsn_1023_02_peloso-piurcosky.pdf. Acesso em: 20 dez. 2023.

REGALADO, Antonio. 23andMe Sells Data for Drug Search. **MIT Technology Review**. 21 jun. 2016. Disponível em: https://www.technologyreview.com/2016/06/21/159352/23andme-sells-data-for-drug-search/. Acesso em: 20 maio 2022.

ROHDEN, Fabíola. Vida saudável *versus* vida aprimorada: tecnologias biomédicas, processos de subjetivação e aprimoramento. **Horizontes Antropológicos**, Porto Alegre, v. 23, n. 47, p. 29-60, jan.-abr. 2017. DOI: http://dx.doi.org/10.1590/S0104-71832017000100002. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.br/j/ha/a/NHHX5NcL4yFYXNX88msZyXh/?format=pdf. Acesso em: 15 fev. 2023.

RONCOLATO, Murilo. O vazamento de dados do MyHeritage. E a alta dos testes genéticos. **Nexo**, 3 set. 2018. Disponível em: https://www.nexojornal.com.br/expresso/2018/09/03/O-vazamento-de-dados-do-MyHeritage.-E-a-alta-dos-testes-gen%C3%A9ticos. Acesso em: 20 maio 2022.

SBPC. Sociedade Brasileira de Patologia Clínica. **Posicionamento da Sociedade Brasileira de Patologia Clínica/Medicina Laboratorial sobre Testes Genéticos Diretos ao Consumidor (TGDCs)**. *s.d.* Disponível em: http://www.sbpc.org.br/wp-content/uploads/2019/12/TGDCs2019.pdf. Acesso em: 12 fev. 2022.

SEGATA, Jean. A colonização digital do isolamento. **Cadernos de Campo**, São Paulo, v. 29, n. 1, p. 163-171, 2020. DOI: https://doi.org/10.11606/issn.2316-9133.v29i1p163-171. Disponível em: https://www.revistas.usp.br/cadernosdecampo/article/view/171297. Acesso: 10 fev. 2023.

UNIÃO EUROPEIA. Regulations. General Data Protection Regulation. **Official Journal of the European Union**. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 14 maio 2022.

ZORZETTO, Ricardo; FIORAVANTI, Carlos. Sérgio Pena: sob a pele. **Pesquisa FAPESP**, n. 306, ago. 2021. Disponível em: https://revistapesquisa.fapesp.br/sergio-pena-sob-a-pele/. Acesso em: 15 maio 2022.

https://doi.org/10.29397/EdicoesLivres/20250105

Recodificando a terapia: um estudo de caso do aplicativo Cíngulo

Fernanda Bruno
Paulo Faltay
Paula Cardoso Pereira
Helena Strecker
Manuela Caputo

Os dados sobre a saúde das pessoas há tempos deixaram de se limitar aos registros médicos e às bases de dados geridas por laboratórios clínicos ou por instituições voltadas para a promoção e o cuidado com a saúde. Para além da expansão da telemedicina e da digitalização dos dados e dos serviços de saúde, que envolvem uma gama cada vez mais vasta de dispositivos inteligentes e equipamentos conectados, um processo mais amplo e difuso de "datificação da saúde"[1] está em curso. Esse processo envolve tecnologias digitais de uso massivo e cotidiano que convertem uma série de comportamentos e processos físicos ou fisiológicos em dados que permitem informar ou inferir estados e aspectos da saúde de indivíduos e populações, tornando-os acessíveis para uma série de atores que extrapolam o *setting* clínico. Os limites que definem o que são dados de saúde na cultura digital tornam-se cada vez mais indefinidos, uma vez que a saúde física e a saúde mental tornam-se legíveis em diversos tipos de comportamentos, ações e informações através dessas tecnologias e desses ambientes digitais.

Nesse contexto, nos interessa explorar especialmente a datificação de processos psicológicos e emocionais. Para tanto, nos voltamos para aplicativos móveis orientados para a saúde mental e o bem-estar psíquico.[2] Esses aplicativos abrangem um escopo heterogêneo de serviços e funcionalidades: desde técnicas de meditação, passando por controle do sono e outras funções fisiológicas, técnicas de apoio emocional e psicológico, até a realização de testes psicológicos ou o acompanhamento terapêutico. Focalizamos, nesse escopo, o que designamos

1 O termo datificação designa, em linhas gerais, a conversão de aspectos da vida cotidiana em dados quantificados (Mayer-Schönberger; Cukier, 2013; Van Dijck, 2014). Quanto à "datificação da saúde", adotamos, neste artigo, a definição mais ampla, proposta no relatório publicado pelo Ada Lovelace Institute: "In the context of health, datafication is the process where individuals' activity, behaviour and experiences are recorded in quantified data and made analysable by an array of actors in and beyond clinical settings, as reference points for health" (2020, p. 6). Para uma análise dessa noção no âmbito das práticas clínicas e de autocuidado, ver Ruckenstein; Dow Schüll, 2017.

2 Os aplicativos móveis (apps) relacionados à saúde (*mobile health* ou *mhealth*, em inglês) pertencem a um campo em plena expansão na economia da conectividade móvel. No amplo espectro de aplicativos orientados para o bem-estar e para a saúde, observamos um crescente interesse por aqueles voltados para a saúde mental e o bem-estar psíquico (WHO, 2020).

como "aplicativos de autocuidado psicológico" ou, numa versão abreviada, PsiApps. Tal designação provém do modo como os próprios apps enunciam o serviço que oferecem, bem como os estados de bem-estar psicológico que dizem promover.

Atrelados a infraestruturas de dados e a modelos econômicos de plataformas digitais, os aplicativos móveis alimentam mecanismos de coleta, armazenamento, análise, predição e uso de dados comportamentais. Esse ecossistema digital entrelaça, de modo singular, corporações de tecnologia, ciência e sociedade em uma nova lógica que investe, cada vez mais, em processos algorítmicos de captura, análise e uso de informações psíquicas e emocionais extraídas de grandes volumes de dados.

Tendo em vista compreender como as informações psicológicas e emocionais vêm sendo coletadas e usadas em aplicativos móveis, a pesquisa sobre os PsiApps, realizada entre agosto de 2019 e junho de 2022, foi estruturada em duas etapas. A primeira selecionou e analisou dez aplicativos de saúde mental de maior popularidade e relevância no Brasil, focalizando, de um lado, os discursos que os próprios aplicativos promovem nas lojas de apps, *sites* e redes sociais e, de outro, o ecossistema de dados (mecanismos de coleta e compartilhamento de dados do usuário) que tais aplicativos integram e alimentam.[3]

A segunda etapa da pesquisa, apresentada e analisada nesse artigo, se concentrou no app Cíngulo, que se define como um aplicativo de "terapia digital" ou "terapia guiada", com o qual "você pode resolver as questões emocionais que mais atrapalham a sua vida e se aprimorar pelo autoconhecimento". Um dos PsiApps mais utilizados no Brasil e eleito pelo Google como melhor aplicativo em 2019, o Cíngulo foi o aplicativo que se mostrou mais relevante, segundo os critérios que orientaram o mapeamento dos aplicativos de saúde mental mais populares no Brasil[4] realizado na primeira etapa da pesquisa (Bruno; Bentes; Antoun *et al.*, 2020).

Ainda, na segunda etapa da pesquisa, buscamos compreender as funcionalidades do aplicativo e o tipo de experiência que busca promover no usuário, bem como as avaliações explícitas que os usuários fazem do app. Para tanto, exploramos dois eixos de análise. O primeiro consistiu na "análise preliminar

3 Para os resultados da primeira etapa, confira Bruno; Bentes; Antoun *et al.*, 2020 e Bruno; Pereira; Bentes *et al.*, 2021. As duas etapas da pesquisa sobre os PsiApps são parte do projeto "Economia psíquica dos algoritmos: racionalidade, subjetividade e conduta em plataformas digitais", coordenado por Fernanda Bruno e desenvolvido no MediaLab. UFRJ, com apoio do CNPq. Cf. Bruno, 2018; Bruno; Bentes; Faltay, 2019. Disponível em: https://medialabufrj.net/projetos/economia-psiquica-dos-algoritmos-racionalidade-subjetividade-conduta-em-plataformas-digitais/. Acesso em: 12 jan. 2024.

4 O mapeamento e rankeamento dos dez aplicativos de saúde mental seguiu os critérios de: 1) relevância para a pesquisa (menção a ferramentas de monitoramento de estados psíquicos, humor e/ou emoções; e 2) popularidade (somente foram selecionados aplicativos com mais de 5 mil avaliações na Google Play Store) (Bruno; Bentes; Antoun *et al.*, 2020; Bruno; Pereira; Bentes *et al.*, 2021).

dos comentários" das(os) usuárias(os) do Cíngulo na Google Play Store, a loja de aplicativos da Google, de forma a compreender, a partir das avaliações das(os) usuárias(os), aspectos da experiência de uso do aplicativo. O segundo buscou simular a "jornada de usuária", isto é, a trajetória que uma pessoa efetua ao baixar, abrir e utilizar o aplicativo. Analisamos, assim, de forma mais detalhada as funcionalidades e o conteúdo do Cíngulo, bem como a experiência personalizada de autoconhecimento e a terapia digital que o app promove na sua oferta de bem-estar mental e emocional. Nesse eixo, foram exploradas apenas as funcionalidades gratuitas do aplicativo.[5]

Inspirando-nos em metodologia elaborada no campo de estudos sobre aplicativo (*app Studies*), exploramos a jornada simulando três *personas* marcadamente distintas, de modo a observar como o aplicativo responderia a diferentes usos e perfis emocionais de usuário.[6] Três pesquisadoras realizaram esse processo, simulando:

1) uma *persona* com baixo bem-estar emocional, que respondeu ao teste de autoavaliação com as opções mais extremas, caracterizando-se como muito desmotivada, pessimista, teimosa, irritada, impaciente, tensa, ansiosa etc.;

2) uma *persona* com médio bem-estar emocional, que selecionou a opção média em todas as questões do teste;

3) uma *persona* com alto bem-estar emocional, que selecionou as opções do extremo oposto à primeira *persona*, caracterizando-se como muito otimista, motivada, flexível, relaxada, prudente etc.

Além da análise dos comentários e da jornada da usuária, foram realizadas duas entrevistas, uma com um *designer* de produto digital, outra com um funcionário do Cíngulo, visando uma melhor compreensão tanto do processo de concepção de um app quanto da percepção da própria empresa sobre seu produto.

O estudo detalhado do Cíngulo, a partir dos dois eixos de análise, nos permitiu identificar importantes aspectos da experiência da(o) usuária(o) e do modo como o aplicativo oferece uma trajetória supostamente personalizada em direção ao bem-estar psicológico e emocional, cujos destaques sistematizamos a seguir. Na análise dos comentários da Google Play Store, identificamos uma quase unanimidade de elogios ao app, sobretudo em relação à precisão da análise de

5 De caráter *freemium* (*free + premium*), o Cíngulo reserva uma série de conteúdos exclusivamente para usuários *premium*. O valor do plano anual do aplicativo é R$199,90.

6 Ver: Multi-Situated App Studies: Methods and Propositions (Dieter; Gerlitz; Helmond *et al.*, 2019).

personalidade da ferramenta de autoavaliação. Já no mapeamento da experiência de uso do app, percebemos que as promessas de personalização enunciadas por seus promotores não se concretizam e que existe grande semelhança entre o questionário utilizado na autoavaliação e o Modelo de Temperamento Afetivo e Emocional (Affective and Emotional Composite Temperament – AFECT) em que se baseia, criando uma zona nebulosa de extração e utilização de dados psicológicos e emocionais.

Além disso, nas Sessões de Autoconhecimento e Técnicas SOS, notamos a presença de um entendimento computacional da mente e de promessas de recodificação das subjetividades, através das ferramentas ofertadas. Essa recodificação, segundo o app, pode ser otimizada, mediante práticas de treinamento de si que convertem a(o) usuária(o) em uma interface programável para se tornar mais produtiva(o) no trato das atividades e nas emoções cotidianas. Prevalece, em toda a jornada da usuária, um modelo de bem-estar psicológico e emocional centrado na individualidade e na autonomia, ressoando modos de subjetivação neoliberais e das múltiplas formas de cisão relacional que ele instaura.

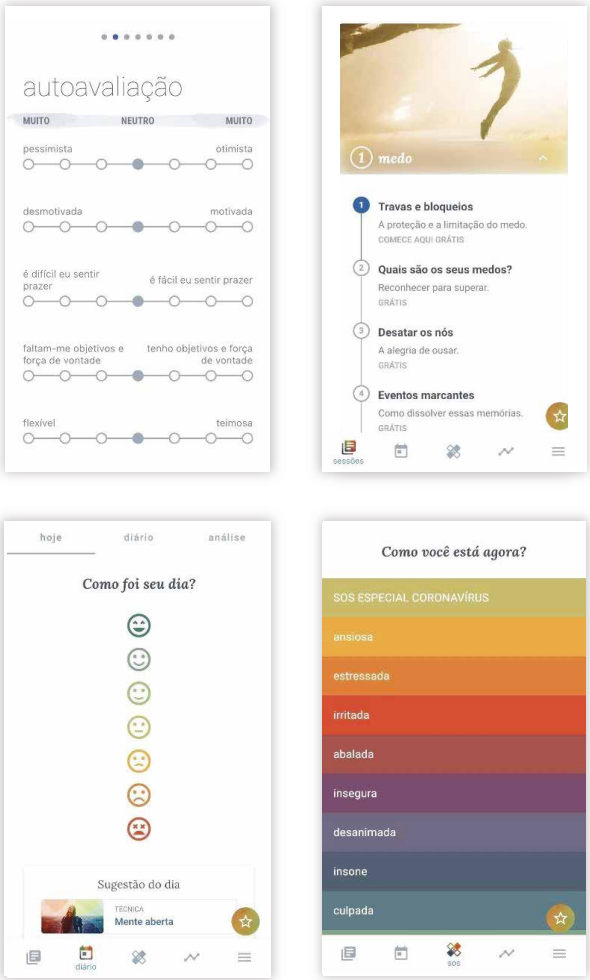
Por fim, ressaltamos que a terapia digital proposta pelo Cíngulo materializa sintomaticamente uma série de reconfigurações das práticas terapêuticas, num contexto de digitalização e datificação de múltiplas esferas da vida. Alinhada ao ideal da "não fricção" que orienta o *design* de experiência do usuário na indústria digital, a "terapia sem fricção", ofertada pelo Cíngulo, tende a ser um processo fluido, imediato, otimizável, confortável e veloz. Como contraponto a esse modelo, propomos uma abordagem metodológica em que as jornadas das usuárias produzam atrito e estranhamento, nas quais deveria haver automatismo e otimização, dando relevo ao que o app visa construir como uma experiência fluida e simples. Nesse sentido, trata-se de uma (contra)jornada que abre espaço para inquietações e reflexões, em vez de simplesmente simular a trajetória de uma usuária abstrata.

Nos itens que se seguem, realizamos uma breve apresentação do aplicativo Cíngulo, seguida da análise dos dois eixos de investigação mencionados e das considerações finais.

1. O Cíngulo

O aplicativo Cíngulo é constituído pelas seguintes funcionalidades:

Figura 1 - Funcionalidades do Cíngulo



Autoavaliação: "A cada duas semanas você poderá refazer a autoavaliação que acabou de fazer e comparar a evolução do seu desempenho emocional".

Sessões de Terapia Guiada: "Aqui você pode aprofundar seu autoconhecimento em sessões com conteúdos e práticas. Que tal começar por aqui?".

Técnicas SOS: "Aqui você pode acessar práticas para lidar rapidamente com situações críticas como ansiedade e estresse".

Diário Emocional: "Preenchendo seu diário, você pode entender o que te faz bem e o que te faz mal no dia a dia e refletir sobre seus aprendizados".

As funcionalidades mais acessadas pelas(os) usuárias(os), conforme constatamos nos comentários na Google Play Store e em entrevista com um profissional da equipe de desenvolvedores do app, são: a Autoavaliação, as Sessões de Terapia Guiada e as Técnicas SOS. Na jornada do aplicativo, exploramos essas três funcionalidades principais.

2. A avaliação da(o) usuária(o) na Google Play Store

A fim de compreender a opinião de quem utiliza o aplicativo, efetuamos análises quantitativas e qualitativas das resenhas publicadas sobre o Cíngulo, na Google Play Store.[7] Nessa loja, cada aplicativo ofertado tem uma página contendo as principais informações sobre o produto, além das avaliações das(os) usuárias(os) sobre o app. As avaliações apresentam-se em dois níveis: a avaliação em escala de 1 a 5 estrelas, sendo 5 a nota máxima, e a avaliação por escrito, disponível na seção "Resenhas" da página de cada produto. As(os) usuárias(os) não são obrigadas(os) a efetuar nenhuma das avaliações, no entanto, a avaliação por estrela é um pré-requisito para aqueles que desejam publicar a avaliação por escrito.

No caso do Cíngulo, a preponderância das avaliações positivas é patente, logo no primeiro nível, uma vez que o app tem nota média de cinco estrelas, o que foi confirmado na análise das resenhas. Para coletar os dados da página do Cíngulo na loja da Google e o conteúdo das resenhas de forma integral, contamos com o auxílio de recursos e ferramentas de automatização. Desde a coleta das resenhas até a filtragem e análise quantitativa dos dados, foram utilizados um *script* em linguagem de programação Python, o aplicativo de análise de texto Voyant Tools e o programa DB Browser. Realizamos uma raspagem dos dados em 10 de maio de 2021, que resultou na coleta de 51.895 resenhas publicadas até essa data.[8]

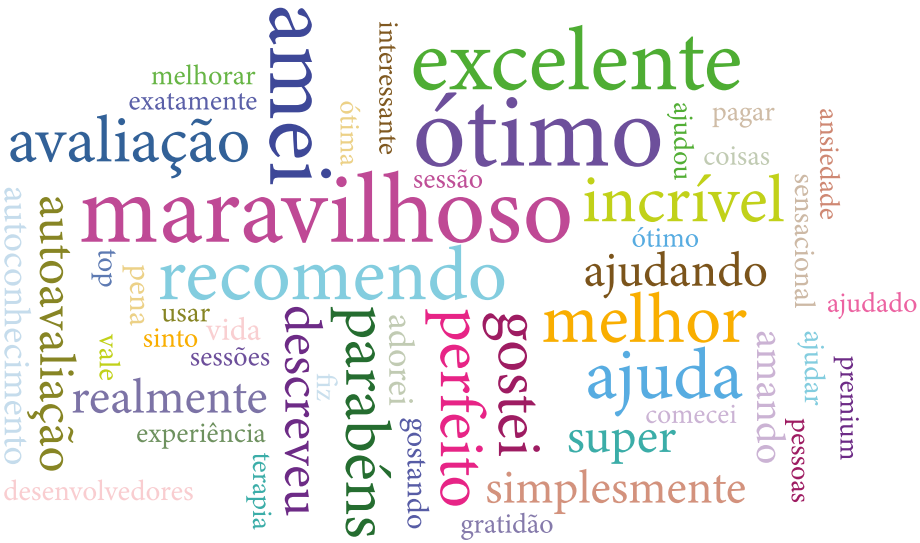
As resenhas foram agrupadas de acordo com a avaliação em estrelas que as acompanhavam e constatamos que a avaliação máxima é quase unânime entre aqueles que também opinaram sobre o Cíngulo por escrito: 49 mil ou 94,4% desses

7 Disponível em: https://play.google.com/store/apps/details?id=com.cingulo.app&hl=pt_BR&gl=US. Acesso em: 10 jan. 2024.

8 Para a raspagem de dados, executamos um *script* em Python, no Google Colab. Disponível em: https://github.com/JoMingyu/google-play-scraper. Acesso em: 15 jan. 2024. Os dados foram reunidos em arquivo .csv e analisados no DB Browser SQLite.

usuários avaliaram o app com 5 estrelas. A análise de conteúdo das resenhas foi realizada inicialmente no Voyant Tools, tendo em vista identificar os termos mais recorrentes nas avaliações das(os) usuárias(os). Essa análise reforça a aprovação do Cíngulo por parte das(os) usuárias(os) diante do elevado número de palavras com conotação positiva – "ótimo, maravilhoso, excelente, amei e recomendo" –, tendência presente até o 100° termo mais recorrente, aproximadamente. A nuvem de palavras abaixo contém os termos mais presentes nas resenhas.[9]

Figura 2 - Nuvem de palavras, coletadas na Google Play Store, com os termos mais recorrentes nas resenhas sobre o Cíngulo



Entre as dez palavras mais recorrentes, o único termo que não é um elogio direto ao aplicativo é "avaliação". O termo se destaca, pois faz referência à funcionalidade de autoavaliação do aplicativo, sendo essa a funcionalidade do app mais citada nas resenhas. Os comentários evidenciam, assim, a centralidade da autoavaliação para o sucesso do aplicativo, uma vez que a ferramenta é constantemente citada de forma elogiosa e qualificada como precisa. Também são comuns as avaliações de pessoas que se tornaram usuárias do aplicativo há poucos dias, mas já afirmam ter obtido resultados do app, relativos ao bem-estar emocional, como a redução da ansiedade e o aumento da autoestima.

9 Após a ordenação automatizada pela frequência com que as palavras aparecem no *corpus*, realizamos uma edição manual da lista de termos, excluindo palavras que não tinham relevância para a análise.

3. Uma (contra)jornada da usuária

Ao abrir o Cíngulo, pela primeira vez, cada usuária precisa criar uma conta, podendo utilizar um *e-mail*, conta do Google ou da Apple. Nesse momento, o app convida a usuária a descrever o nome e pronome com que deseja ser chamada e já inicia a sua retórica de personalização. O nome ou apelido indicado é utilizado durante todo o uso do Cíngulo, buscando criar um vínculo íntimo que se sobreponha (ou até faça esquecer) o caráter maquinizado do cuidado oferecido.

3.1 Autoavaliação: autoconhecimento automatizado e falhas na personalização

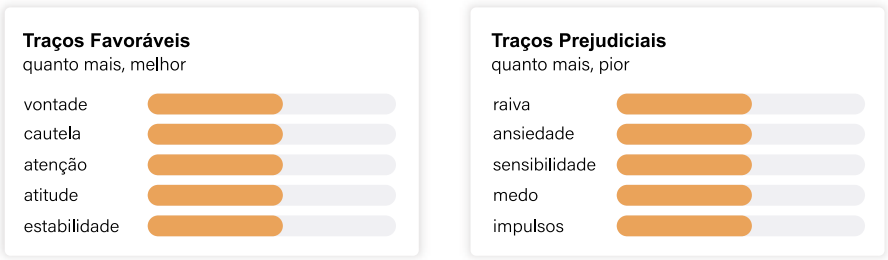
A autoavaliação, apresentada como "um teste rápido para iniciar seu caminho de autoconhecimento", é a primeira etapa de uso do aplicativo, obrigatória para acessar as outras ferramentas do Cíngulo. Ao longo do processo de autoavaliação, identificamos alguns elementos que merecem destaque e que detalhamos a seguir.

O primeiro elemento a ser detalhado são as falhas na abordagem personalizada ofertada pelo aplicativo, em geral, e pela autoavaliação, em particular. Na ferramenta de autoavaliação, a usuária é convidada a "conhecer seu perfil emocional, pontos fortes e fracos" em um questionário objetivo de 36 itens e uma escala de sete opções de resposta (que variam entre pouco, neutro e muito). Seguindo a metodologia das três *personas*, descrita anteriormente, cada usuária respondeu ao teste, de acordo com a sua *persona*.

Ao final da autoavaliação, cada uma recebeu sua nota de "mental *fitness*". A *persona* com alto bem-estar emocional recebeu a nota 10; a com médio bem-estar emocional, 5; e a com baixo bem-estar emocional ficou com nota 0, complementada pela mensagem de que seria recomendável procurar acompanhamento profissional de psicólogo ou psiquiatra. O aplicativo estimula a realização da autoavaliação de forma periódica (a cada duas semanas), para que a(o) usuária(o) acompanhe a evolução do seu desempenho emocional.

Além da nota, a usuária recebe uma escala que apresenta quais são seus "traços favoráveis" ("quanto mais, melhor") e "traços prejudiciais" ("quanto mais, pior"). A *persona* com alto bem-estar emocional recebeu 100% de traços favoráveis; a com baixo bem-estar emocional recebeu 100% de traços prejudiciais; e a com médio bem-estar emocional ficou com 50% em todos os traços. Essa escala de traços fornece pistas de qual seria o perfil emocional "ideal" para o Cíngulo, como podemos ver na imagem abaixo:

Figura 3 - Escala de traços favoráveis e desfavoráveis apresentada ao final da autoavaliação



Ao final da autoavaliação, o Cíngulo apresenta uma análise completa das características emocionais da usuária, retomando os itens do questionário em um texto que pretende soar personalizado, mas que certamente é automatizado, materializando uma espécie de "diagnóstico maquínico". Referindo-se ao sujeito sempre na segunda pessoa, o texto faz uma série de afirmações sobre a personalidade e os modos de levar a vida de cada usuária, inferindo aspectos sobre suas emoções, suas ações e seus jeitos de se relacionar. É explícita a intenção de utilizar uma linguagem personalizada, ao tentar expressar certa proximidade e intimidade com o sujeito.

Em alguns momentos, as considerações se aproximam do diagnóstico, com frases incisivas sobre o perfil emocional de cada uma, como: "poucas coisas lhe dão prazer" e "seu perfil é de quem se magoa com facilidade, se culpa demais, lida mal com a rejeição e teme ser abandonada pelas pessoas da sua vida" – isso para a primeira *persona*. Simultaneamente, o texto promove as funcionalidades do aplicativo, exaltando como elas podem ajudar a usuária a solucionar os problemas identificados no próprio texto.

A tabela abaixo reproduz trechos das análises recebidas pelas usuárias. Destacamos esses trechos porque, apesar das três *personas* terem respondido à autoavaliação de forma extremamente distinta, uma vez que simulam "personalidades" e "perfis emocionais" díspares, elas receberam textos extremamente similares, evidenciando uma clara falha na personalização promovida pelo aplicativo.

Tabela 1 - Trechos das análises recebidas pelas usuárias, ao final da autoavaliação

Alto bem-estar emocional	Médio bem-estar emocional	Baixo bem-estar emocional
Sua **necessidade de saciar desejos** é **moderada**, o que pode levar a alguns comportamentos demasiados em áreas como compras, sexo, drogas e/ou comida. Às vezes você exagera no que gosta, podendo bater algum arrependimento mais tarde sobre o que fez.	Sua **necessidade de saciar desejos** é **moderada**, o que pode levar a alguns comportamentos demasiados em áreas como compras, sexo, drogas e/ou comida. Às vezes você exagera no que gosta, podendo bater algum arrependimento mais tarde sobre o que fez.	Sua **necessidade de saciar desejos** é **intensa**, com grande propensão a comportamentos compulsivos em alguma área como compras, sexo, drogas e/ou comida. Quando seu impulso surge, muitas vezes do nada, é difícil controlá-lo. Sua tendência é exagerar para só depois se arrepender do que fez.

Como se pode notar, a *persona* com alto ou médio bem-estar emocional recebeu exatamente o mesmo "diagnóstico", enquanto a *persona* com baixo bem-estar emocional recebeu uma análise mais contundente, mas muito similar.

Além da similaridade entre os textos da autoavaliação, foram sugeridas para as três *personas* as mesmas Sessões de Autoconhecimento, na mesma ordem. É interessante observar como essas falhas flagrantes na personalização anunciada pelo app são contraditórias com o inegável "sucesso" que a autoavaliação faz junto às(aos) usuárias(os). Ou seja, o fato de que o texto, na prática, pouco tenha de personalizado não impede que seja assim percebido pelas(os) usuárias(os). Como aponta um dos comentários na loja da Google: "Muito perfeito o app, a avaliação parece de alguém que me vigia *rs* chorei na primeira sessão, simplesmente maravilhosa".

A recorrente alusão à precisão descritiva do texto da autoavaliação articula-se com o segundo elemento que ressaltamos acerca dessa funcionalidade: o fato de que ela opera como um mecanismo forte e imediato de conquista e retenção das(os) usuárias(os). Como descrito no tópico 2, um número expressivo de comentários na Google Play Store afirmam que a autoavaliação definiu a personalidade com precisão ou ajudou as pessoas a compreenderem melhor a si mesmas. Conforme relato de um funcionário do Cíngulo, em entrevista, essa é uma das funcionalidades que mais gera engajamento, apontada como uma das grandes responsáveis pela satisfação expressa das(os) usuárias(os).

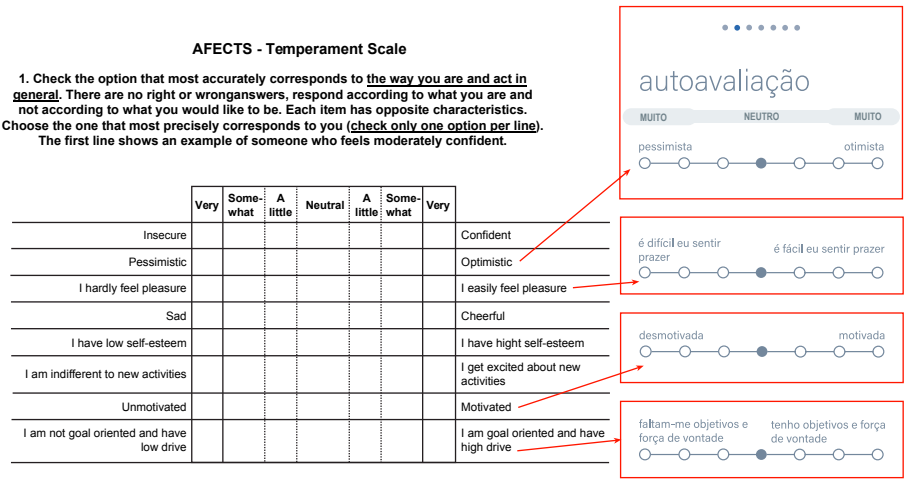
O terceiro elemento a ser destacado em relação à autoavaliação é a semelhança entre o questionário utilizado e o modelo AFECT (acrônimo de Affective and

Emotional Composite Temperament, Modelo de Temperamento Afetivo e Emocional), criado e validado pelos fundadores do app e sobre o qual trataremos a seguir. Importante ressaltar que o AFECT, no entanto, não é mencionado nem no fluxo de uso do aplicativo, durante a autoavaliação, nem nos Termos de uso e Política de privacidade[10], como veremos.

3.1.1 Modelo AFECT e autoavaliação: entre ciência, clínica e autotestagem digital

O AFECT[11] é um modelo e uma escala de avaliação de temperamento afetivo e emocional desenvolvido pelo psiquiatra Diogo Lara, criador do Cíngulo, em parceria com outros pesquisadores. Conforme seus criadores, o modelo é resultado de um esforço em criar um instrumento autoaplicável, curto e válido, o mais simples possível, sem perder o poder explicativo. "Nosso objetivo era criar um modelo com definições claras de saúde e disfunção mental que pudesse ser facilmente aplicado na prática clínica", explicam os autores em um artigo (Lara; Bisol; Brunstein *et al.*, 2012, p. 20).

Figura 4 - Correspondência entre a escala de temperamento AFECT e o questionário utilizado na autoavaliação



10 O Cíngulo adota em seu *site* um único documento para os Termos de uso e Política de privacidade, chamado de Termos de Uso e Condições Gerais do Serviço. Neste texto, chamaremos o documento de Termos de Uso. A última versão dos Termos de uso é de 8 de fevereiro de 2022. Disponível em: https://accounts.cingulo.com/terms.html?aid=&as=&lang=pt-BR. Acesso em: 4 abr. 2022.

11 O Modelo de Temperamento Afetivo e Emocional (Affective and Emotional Composite Temperament – AFECT) é uma abordagem que integra emoção, comportamento, cognição e personalidade. O modelo parte do pressuposto de que o temperamento é um elemento-chave para entender a saúde mental e as patologias. No AFECT, existem dois vetores emocionais básicos, a Ativação (concebida como vontade e raiva) e a Inibição (representada pelo medo e pela cautela). Além desses vetores, as outras dimensões que compõem o substrato emocional básico, segundo o modelo, são Sensibilidade e Coping, que determinam como o sistema emocional reage ao ambiente, e o Controle, que monitora o ambiente e faz ajustes na Ativação e na Inibição. A interação entre essas dimensões básicas resulta em perfis de temperamento que se aproximam ou se distanciam da matriz (Lara; Bisol; Brunstein *et al.*, 2012). Os desenvolvedores do Cíngulo em textos científicos e nas redes institucionais de divulgação do app ora nomeiam o modelo como AFECT, ora como AFECTS. Optamos por utilizar apenas AFECT, de modo a padronizar a nomenclatura.

Como se pode ver nas imagens, há uma grande correspondência entre a autoavaliação do Cíngulo e o modelo AFECT: dos 36 itens que compõem a autoavaliação, 29 são iguais aos da primeira parte da escala AFECT. Além disso, na versão do aplicativo, o teste é mais curto[12], o que provavelmente facilita a adesão e a posterior retenção das(os) usuárias(os), bem como o processamento algorítmico dos dados para a elaboração da análise automatizada dos resultados.

Como indicamos anteriormente, não há nenhuma menção durante o uso do app ao fato de que a autoavaliação se baseia nessa escala de temperamento, assim como não há menção aos termos "teste", "autoavaliação" ou "AFECT" nos Termos de uso. Visto que a avaliação psicológica é uma competência de profissionais de psicologia, regulamentada pelo Conselho Federal de Psicologia, a escolha do nome autoavaliação e a decisão de não mencionar o AFECT no aplicativo chama atenção. A única referência explícita que encontramos ao modelo foi em uma publicação do perfil oficial do aplicativo no Instagram, que ressalta a "precisão" da autoavaliação, reproduzindo o bordão comumente usado para enaltecer a capacidade de algoritmos conhecerem as pessoas: "Dizem até que o Cíngulo as conhece melhor do que as próprias mães ou até mais do que elas mesmas".

Figura 5 - *Post* do perfil do Cíngulo no Instagram, no qual se deixa explícita a relação com o modelo AFECT.

12 Enquanto a autoavaliação do Cíngulo tem 36 itens, o AFECT tem 48 itens.

Ainda que não haja menção explícita às palavras listadas acima, os Termos de uso mencionam que os dados de usuárias(os) poderão ser utilizados para "gerar conhecimento científico e aprimorar os produtos do *site*/aplicativo". Além disso, os Termos também admitem a coleta de "traços de sua personalidade que identificam sua saúde mental", classificados como dados sensíveis segundo a Lei Geral de Proteção de Dados Pessoais (LGPD). Isso chama a atenção, uma vez que o próprio AFECT foi desenvolvido e testado, a partir de uma base de dados coletada na internet (o Temperamento: sistema de avaliação mental – www.temperamento.com.br –, *site* lançado em 2011).[13] Essa trajetória evidencia um interesse antigo dos criadores em articular saúde mental e tecnologia, no desenvolvimento de modelos de personalidade, a partir de dados digitais ou de ferramentas tecnológicas de cuidado terapêutico.

Considerando que a autoavaliação possibilita a captura de dados sensíveis sobre características psicológicas e emocionais, bem como a importância de a usuária consentir com a coleta e o uso de seus dados, de forma plenamente informada, a menção ao AFECT nos Termos de uso seria, no mínimo, desejável. Além disso, vale questionar o quanto não deveria haver mais transparência nesse tipo de iniciativa, que se situa na fronteira entre o comercial e científico.

Casos, como o da Cambridge Analytica/Facebook[14], mostraram como essa fronteira produz brechas legais utilizadas por corporações de tecnologia para realizar experimentos baseados e orientados por protocolos científicos, sem, entretanto, precisarem cumprir as exigências éticas e legais estabelecidas pela comunidade científica para a realização de pesquisas com seres humanos.

Tendo em vista a questionável prática, comum nos "laboratórios de plataforma" (Bruno; Bentes; Faltay, 2019), de realizar inúmeros experimentos psicossociais sem o devido cuidado ético, nos perguntamos se a autoavaliação do Cíngulo não reproduz essa prática. Ou seja, seria uma ferramenta que permite escalar a coleta de dados pessoais, alimentando um instrumento científico sem que os protocolos científicos sejam plenamente aplicados e sem que as(os) usuárias(os) tenham pleno conhecimento dos usos dos seus dados e do contexto mais amplo em que essa autoavaliação se insere.

13 Nesse caso, o *site* deixava claro que se tratava de um sistema criado com fins científicos e que era uma avaliação mental psicológica e psiquiátrica.

14 NE: O escândalo de dados do Facebook–Cambridge Analytica envolveu o uso indevido de dados de até 87 milhões de usuários do Facebook, influenciando a opinião de eleitores em contextos políticos como as eleições de Donald Trump, nos Estados Unidos, em 2016.

3.2 Sessões de Autoconhecimento e Técnicas SOS

Retomando a (contra)jornada, depois de realizar a autoavaliação, as usuárias são apresentadas às Sessões de Autoconhecimento, que consistem em técnicas de terapia guiada, disponíveis em texto e áudio (narrado pelo próprio dr. Diogo Lara). As sessões são apresentadas como "conteúdos e práticas para aprofundar seu autoconhecimento" e agrupadas segundo diferentes temas: medo, autoestima, relacionamentos, autobiografia, estresse, ânimo, insegurança, atitude, ansiedade, foco, raiva, impulsos, resiliência, sono, meditação I e II. Novamente, como já apontamos, fica evidente a falha na retórica de personalização do app. Apesar de o Cíngulo sugerir que as sessões aparecem em uma sequência personalizada, de acordo com a autoavaliação, as três *personas* simuladas receberam as sessões na mesma ordem. Como utilizamos na pesquisa apenas as funcionalidades gratuitas do aplicativo, somente as cinco primeiras sessões da série medo ficaram disponíveis.[15]

O Cíngulo também oferece às usuárias uma série de Técnicas SOS, apresentadas como "práticas para lidar rapidamente com situações críticas". A partir da pergunta "Como você está agora?", o Cíngulo sugere conteúdos para lidar com situações de ansiedade, estresse, irritação, insegurança, desânimo, insônia, culpa, desatenção e até mesmo um SOS Especial Coronavírus. São oferecidas oito técnicas para cada estado emocional, sendo quatro delas de acesso gratuito e quatro restritas às(aos) usuárias(os) *premium*. Através de conteúdos em texto e áudio, as práticas consistem em exercícios de relaxamento, respiração e terapia guiada, também narrados por Diogo Lara.

Analisando o discurso do aplicativo, nas sessões e nas técnicas, identificamos alguns temas, termos e aspectos recorrentes. Detalhamos a seguir cinco desses aspectos relacionados ao modelo de mente e de subjetividade, ao entendimento de bem-estar psicológico e emocional e ao tipo de experiência terapêutica que estão na base do aplicativo e que norteiam as práticas de cuidado de si por ele propostas.

3.2.1 Código da mente

A concepção da mente como aparato computacional é marcante nas Sessões de Autoconhecimento e nas Técnicas SOS. Chama atenção a recorrência do termo "código" e de metáforas computacionais para se referir a processos psíquicos:

15 Nas Técnicas SOS, diversos conteúdos também são reservados às(aos) usuárias(os) pagantes.

"código da vontade", "código da mente", "arquivo da memória" e, especialmente, a noção de "processamento" para se referir à elaboração de estados emocionais.

"Mergulhe nas cenas, emoções, sensações e pensamentos e deixe acontecer, sua mente fará o processamento de modo natural e automático através da 'inteligência do corpo'." (Técnica PREP – Ansiedade)

Na técnica Imersão, para "processar conteúdos relacionados ao luto", na parte do SOS Especial Coronavírus, há os seguintes trechos:

"Os sons que você ouve só ajudam a processar tudo que está acontecendo aí dentro" (Técnica Imersão – SOS Especial Coronavírus).

Encontramos exemplos desse tipo de abordagem em duas técnicas registradas. A primeira é a de Recondicionamento da Mente pelo Relaxamento (RMR®), anunciada como "uma maneira de deixar sua mente subconsciente mais permeável a mudanças".

"O som bilateral, que você ouve, faz com que esse novo registro penetre de modo profundo e consistente no seu subconsciente. [...] A sua mente agora carrega o código da vontade alta e, portanto, ela é permanente e absolutamente natural para você" (Técnica RMR – Vontade).

A segunda técnica é o Processamento e Recodificação das Emoções e Pensamentos ligados à Ansiedade (PREP®), cujo nome faz claro uso da linguagem computacional.

"Aproveite qualquer emoção mais forte no seu cotidiano para vasculhar seu passado com PREP buscando situações parecidas. Várias dessas experiências podem estar no mesmo arquivo da sua memória e você pode processá-las à medida que vai ouvindo o áudio."

Além de tratar as emoções como "conteúdos a serem processados" (Técnica Imersão), outro ponto a ser destacado é o fato de o app incitar a(o) usuária(o) a se relacionar quantitativamente com seus estados emocionais. Por exemplo, a Técnica PREP – Ansiedade propõe à(ao) usuária(o) mentalizar uma frase positiva que represente a superação da situação de dificuldade trabalhada. Ao final, a(o) usuária(o) deve comparar, em termos percentuais, o quanto acredita na frase antes e depois de realizar a técnica, sendo que o app explicita que "o objetivo é de 80% ou mais" de concordância com a frase.

3.2.2 Reset

O entendimento computacional da mente se expressa também no modo como o app propõe transformá-la: tal como um dispositivo computacional, a mente pode ser "resetada", conforme disciplina, foco e treinamento do sujeito. Nesse sentido, parece haver uma tensão ou ambiguidade. Por um lado, temos o uso de técnicas que "convocam" instâncias que estão fora da consciência; e, por outro lado, temos a pressuposição de um sujeito capaz de controlar e instrumentalizar tais instâncias para fazer uma reprogramação mental de si mesmo.

Por meio desse mecanismo de recodificação ou reprogramação, afirma-se que esse sujeito é capaz de se libertar dos traumas, das dores, das memórias de sofrimento e "promover mudanças profundas em condicionamentos subconscientes". Tudo pode ser repaginado, desfeito, abandonado, superado, reiniciado por meio de técnicas rápidas e eficazes ofertadas pelo próprio aplicativo.

Essa dimensão fica especialmente evidente nas duas técnicas anteriormente citadas – RMR e PREPR, cujas marcas estão registradas pelo app – que são aplicáveis a distintas emoções e diversos sentimentos: ansiedade, estresse, sensibilidade etc.

Já outra técnica, também citada pelo aplicativo, a BSUR (be as you are), é literal na proposta de um "reset" mental. Apresentada como uma técnica para resolver frustrações, mágoas e memórias traumáticas, ela promete "resetar a energia do seu corpo". Para isso, "bastam 6 minutos para lidar com lembranças que têm lhe abalado e mudar o seu estado negativo para um positivo".[16]

O modelo de mente cuja transformação está sob total controle do indivíduo também é notável na técnica Recrutamento Neuronal, que convida a usuária a "acionar a parte frontal do seu cérebro", para alcançar mais concentração, disciplina e produtividade:

> Vão ser três pulsos de energia e luz que vão recrutar todos os seus neurônios para trabalharem na potência máxima. [...] E a cada vez que você faz essa ferramenta, o seu cérebro se habitua a ser mais organizado, disciplinado, responsável, atento e focado. E isso lhe gera uma sensação enorme de satisfação e orgulho. (Técnica Recrutamento Neuronal).

16 Trecho de *post* do Instagram sobre a técnica BSUR: https://www.instagram.com/p/Bue09uXgwDN/.

Essa perspectiva encontra ressonância nas atuais concepções neurobiológicas da personalidade, analisadas por Nikolas Rose (Rose; Abi-Rached, 2013). O autor ressalta o quanto elas estão transformando o modo como conhecemos a nós mesmos e como, curiosamente, não atestam uma determinação ou fatalismo neurobiológico. Ao contrário, anunciam que podemos modificar e melhorar a nós mesmos compreendendo e agindo sobre nossos cérebros.

3.2.3 Mental Fitness

"Como está o seu mental fitness?" A pergunta provoca a usuária a realizar uma nova autoavaliação, incentivada a ser repetida semanalmente e cujo histórico aparece em uma aba chamada "evolução". O Mental Fitness, quantificado numa nota de 0 a 10 para supostamente "medir" o nível de saúde mental da(o) usuária(o), é uma síntese do entendimento de bem-estar psicológico e emocional que está na base do app. A própria utilização do termo em inglês *fitness* remete, simultaneamente, ao exercício, ao treinamento, e àquilo que está em boa condição, bem-adaptado.

Figura 6 - Resultados das autoavaliações das três personas simuladas pela pesquisa. A primeira com baixo nível, a segunda com médio e a terceira com alto bem-estar emocional

O Mental Fitness manifesta um entendimento do cuidado de si e do bem-estar como desempenho emocional, cuja *performance* sempre pode evoluir até o "estágio da plenitude", nos termos do próprio app. A presença de um modelo de autocuidado em que o cuidado de si se transforma num treinamento de si, identificado na primeira fase da pesquisa, ganha nesse contexto contornos muito concretos.

O aprimoramento emocional obedece a uma lógica em que o cuidado constante é sinônimo de contenção do risco potencial de adoecimento ou descuido. As métricas oferecidas pelo aplicativo, associadas aos traços favoráveis e desfavoráveis, determinam os "departamentos" pessoais em que o indivíduo deve investir, a fim de otimizar sua saúde mental, e, consequentemente, refletir positivamente nas atividades e nos relacionamentos da vida dele. Nesse contexto, o próprio usuário se transforma numa interface programável que pode se tornar mais produtiva no manejo das atividades e das emoções cotidianas, embebido de uma lógica neoliberal de produção de subjetividades que atribui, a cada um, a responsabilidade de criar a melhor versão de si mesmo, e a culpa, quando o projeto falha.

3.2.4 Velocidade e otimização

Ao contrário de uma psicoterapia tradicional, em que o tempo é indeterminado, a experiência terapêutica ofertada pelo app promete ter resultados quase imediatos. A mudança psíquica deve ser rápida. Uma veloz otimização de si que promete, inclusive, a chegada ao "estágio da plenitude". Um reset e pronto! A recodificação acelera-se com o uso. "Quanto mais você usar o Cíngulo, mais rápido vai evoluir", avisa-se ao final da primeira sessão ofertada. A repetição aparece aqui não para elaborar e, sim, para engajar e automatizar os comandos.

As notificações, as sugestões e os lembretes que o Cíngulo sugere ativar estimulam o uso diário do aplicativo, incorporando-o como um hábito na rotina do indivíduo. "Quem faz sessões regularmente tem resultados mais rápidos para reduzir o medo, vencer bloqueios e deixar para trás a vergonha e a timidez", diz a mensagem de lembrete das sessões. Também notamos que há um padrão nas notificações, que chegam todos os dias às 9h e às 21h15, início e fim do dia, com frases inspiradoras e sugestões de registrar os acontecimentos do dia no Diário Emocional.

A promessa de velocidade nos efeitos é reiterada em vários momentos das técnicas e sessões, como revela o trecho: "Até o final dessa sessão você será capaz de se manter protegida e segura, ao mesmo tempo que poderá expandir até o estágio da plenitude, se libertando das suas travas, bloqueio e limitações" (Sessão Travas e Bloqueios, da série medo). O próprio nome Técnicas SOS, para lidar com os momentos em que a usuária se sente "culpada", "abalada", "insegura", aponta para a promessa de eficiência e velocidade.

Ainda que tais feitos não encontrem respaldo na psicologia clínica, que, em suas diversas abordagens, é majoritariamente cética em relação a tratamentos rápidos,

a retórica do app é reverberada por comentários das(os) usuárias(os) que também manifestam de forma recorrente a percepção sobre uma melhora rápida:

> Na primeira sessão, já vi que descobri o melhor app da minha vida... Extremamente maravilhoso. Por eu ser uma vítima de ansiedade crônica, na primeira sessão, me senti aliviado. Amei e vou continuar e ainda recomendar para todos. Gratidão a todos vcs. que criaram esse app fantástico.
>
> Me ajudou muito. Nem acreditei no que esse app é capaz. Uma sessão e já senti o fardo mais leve. Além disso, vai me poupar muitos problemas futuros e uma boa economia com psicólogos. Fora a cura da minha ansiedade.

Importante notar como o ideal da otimização também orienta as dinâmicas do próprio aplicativo. Como todos os produtos digitais, ele se atualiza numa lógica de teste e descarte, validação e alteração constantes. Uma funcionalidade que não tenha bom engajamento entre as(os) usuárias(os), normalmente, é desativada, contribuindo, entre outros motivos, para que a abordagem do aplicativo se transforme numa grande "salada teórico-clínica". Contraditoriamente ao discurso que destaca a base científica no desenvolvimento do aplicativo, as funcionalidades que o constituem são definidas muito mais pelo sucesso que fazem entre as(os) usuárias(os) do que por parâmetros de ordem científica ou terapêutica.

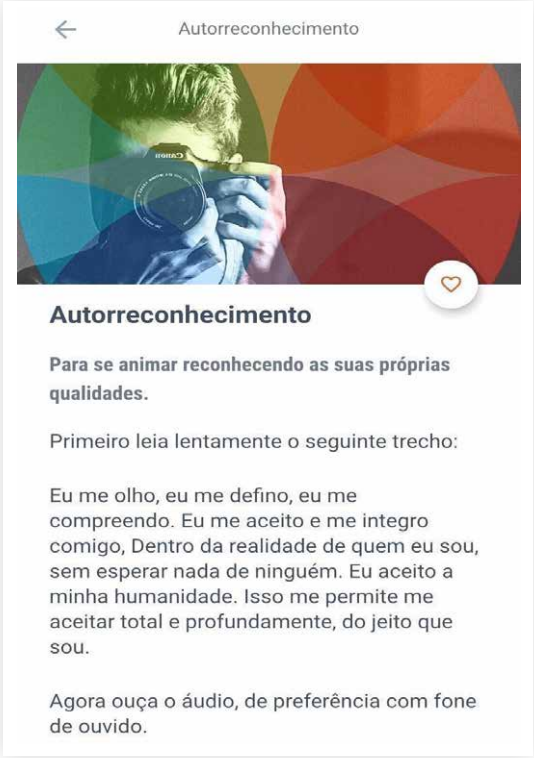
3.2.5 "Autotudo"

Como já havíamos identificado, na primeira fase da pesquisa, as ênfases na individualidade e na autonomia, sintetizadas no ideal do sujeito que faz "tudo por conta própria", adquirem aqui ainda mais dimensões e maior centralidade. Da autoavaliação à autoestima, ao autocuidado, à autogestão, ao autocontrole, ao autorreconhecimento, incluindo até a desconcertante sugestão de um "autoabraço", como forma de autoacolhimento em algumas sessões e técnicas, ressoam modos de subjetivação próprios do neoliberalismo e das múltiplas formas de cisão relacional e sufocamento das práticas do comum que o aplicativo instaura. Nessa oferta incessante de autonomia, poderíamos dizer que o sujeito é incitado, no limite, a ser seu autopsicólogo.

Ainda sobre essa inflação e quase onipresença do prefixo "auto", chama especial atenção a proposta de "Autorreconhecimento", cuja finalidade é apresentada como "para se animar reconhecendo as suas próprias qualidades". Sendo o reconhecimento

um conceito historicamente vinculado às relações intersubjetivas, é, no mínimo curioso, se não constrangedor e sintomático, essa adaptação promovida pelo app: "o foco dessa técnica é que o seu reconhecimento vem de VOCÊ, e não, dos outros".

Figura 7 - Trecho da técnica Autorreconhecimento



4. Considerações finais: terapia sem fricção

Alinhado aos princípios que vêm orientando o *design* de experiência da(o) usuária(o), na indústria digital, de um modo geral, a experiência visada pelos idealizadores de aplicativos é que eles sejam "lisos". Em outras palavras, que eles demandem o menor esforço possível de quem o utilize. A arquitetura da informação, orientada ao engajamento dos aplicativos, almeja produzir um vínculo rápido, em poucos cliques, em poucas ações, contribuindo para as estratégias comerciais de retenção das(os) usuárias(os). O objetivo é que a experiência de uso cause a menor resistência e demande o menor esforço cognitivo possível do sujeito; que a usabilidade do produto

seja fácil, fluida e simples. Essa abordagem vem sendo conhecida, no meio tecnológico, como "*design* sem fricção" (*frictionless design*, em inglês) (Cupples, 2021).

Na experiência da(o) usuária(o), o atrito é definido como "interações que inibem as pessoas de atingir seus objetivos de forma intuitiva e indolor dentro de uma interface digital" (Young, 2015). Eliminar o atrito tornou-se, assim, o foco de um modelo tecnológico (que também é um modelo de negócios) ancorado na cultura da otimização e da velocidade. O *design* sem atrito visa produzir experiências que podem ser sintetizadas sob o princípio proposto por Steve Krug para "melhores práticas" de usabilidade: "não me faça pensar" (Krug, 2005).

Mas quais as implicações, quando o ideal da *não fricção* orienta uma proposta terapêutica, através de um aplicativo? Guiada pela lógica da usabilidade e do engajamento, a experiência psicoterapêutica, tradicionalmente marcada pelo questionamento, pela elaboração, pela complexidade, pelo conflito, pela não linearidade, em suma, pela *fricção*, torna-se, nesse contexto, um processo simplificado, confortável, rápido e fácil.

Alinhada com uma concepção computacional dos processos psíquicos e emocionais, com os ideais de otimização, velocidade e facilidade, assim como de um constante aprimoramento e monitoramento, supostamente autônomo de si, a "terapia sem fricção", ofertada pelo Cíngulo, é sintomática de processos mais amplos que configuram a saúde mental na atualidade. Tais processos incluem a precarização dos serviços de saúde pública, de uma forma geral, e de saúde mental, em particular, a pressão social por soluções rápidas e pouco "custosas" tanto em termos econômicos quanto cognitivos e existenciais, e a intensificação e a "naturalização" do uso de aplicativos e robôs nos serviços de saúde – ocorridas, sobretudo, durante a pandemia de covid-19.

Além disso, tanto os problemas visados pelo app, como as ferramentas através das quais ele se propõe a rapidamente solucioná-los são indissociáveis de um momento histórico em que o sofrimento psíquico não é apenas produzido, mas gerido segundo a lógica neoliberal (Safatle; Silva Junior; Dunker, 2020). Uma vez que a força neoliberal "recodifica identidades, valores e modos de vida por meio dos quais os sujeitos realmente modificam a si próprios, e não apenas o que eles representam de si próprios" (Safatle; Silva Junior; Dunker, 2020, p. 10), o Cíngulo parece integrar perfeitamente um conjunto de técnicas de produção de modos de subjetivação específicos do neoliberalismo.

Entre outras ressonâncias de uma concepção de saúde mental alinhada a tal modelo, ao não se apresentar como uma psicoterapia, mas como "terapia digital",

o Cíngulo – e outros apps similares – ajudam a criar uma cultura terapêutica (Rose, 1990; 2011) que vai contra uma série de princípios que orientam um cuidado coletivo com a saúde mental e que vêm sendo, justamente, eliminados por essa lógica.

Nessa cultura terapêutica, os aplicativos digitais são aliados ideais tanto da individualização do cuidado psicológico e emocional quanto da progressiva datificação da saúde mental. Tanto o estudo de caso do Cíngulo quanto a pesquisa mais ampla sobre os PsiApps revelam que esses dois processos se retroalimentam. Ao mesmo tempo, notamos, nas duas etapas da pesquisa, que: se, por um lado, tais aplicativos promulgam a autonomia e o bem-estar das(os) usuárias(os); por outro lado, eles tendem a retirar cada vez mais o sujeito – com suas ambiguidades, seus conflitos, suas resistências, seus questionamentos – do processo de cuidar de si e do outro.

Na primeira etapa da pesquisa, vimos como a inflação da autonomia, presente no discurso de que a(o) usuária(o) faria "tudo por conta própria" na conquista de seu bem-estar psicológico e emocional, contrasta com a falta de conhecimento, o controle e a agência da(o) usuária(o) acerca do ecossistema de extração e do uso de dados extremamente sensíveis sobre sua vida psíquica, íntima e cotidiana.

A análise do Cíngulo reencontra os ideais de autonomia, de personalização e de otimização fortemente presentes nos enunciados, nas narrativas e nas técnicas terapêuticas propostos. Entretanto, tudo isso convive, curiosamente, com técnicas de usabilidade e de engajamento que conduzem a usuária numa trajetória que atende menos a propósitos terapêuticos e mais a estratégias comerciais de atração e retenção de usuárias(os). Configura-se, assim, uma terapia sem fricção, ou uma terapia guiada por dados, em que o sujeito é reduzido às qualidades gerais do usuário digital.

Referências

ADA LOVELACE INSTITUTE. **The data will see you now**: Datafication and the boundaries of health. Londres, 29 out. 2020. Disponível em: https://www.adalovelaceinstitute.org/report/the-data-will-see-you-now. Acesso em: 27 jun. 2022.

BRUNO, Fernanda. A economia psíquica dos algoritmos: quando o laboratório é o mundo. **Nexo**, São Paulo, 12 jun. 2018. Disponível em: https://www.nexojornal.com.br/a-economia-psiquica-dos-algoritmos-quando-o-laboratorio-e-o-mundo. Acesso em: 12 ago. 2018.

BRUNO, Fernanda; BENTES, Anna; ANTOUN, Mariana; CARDOSO, Paula; FALTAY, Paulo; STRECKER, Helena; MARRAY, Moisés; ROCHA, Natássia. **"Tudo**

por conta própria": aplicativos de autocuidado psicológico e emocional. Relatório parcial da pesquisa. Rio de Janeiro: MediaLab. UFRJ, 2020. Disponível em: https://medialabufrj.net/wp-content/uploads/2020/05/Relatorio_PsiApps_MediaLabUFRJ-1.pdf. Acesso em: 27 jan. 2024.

BRUNO, Fernanda G.; BENTES, Anna C. F.; FALTAY, Paulo. Economia psíquica dos algoritmos e laboratório de plataforma: mercado, ciência e modulação do comportamento. **Revista Famecos**, v. 26, n. 3, p. e33095, 2019. DOI: https://doi.org/10.15448/1980-3729.2019.3.33095. Disponível em: https://revistaseletronicas.pucrs.br/ojs/index.php/revistafamecos/article/view/33095. Acesso em: 1 set. 2020.

BRUNO, Fernanda Glória; PEREIRA, Paula Cardoso; BENTES, Anna Carolina F. *et al*. "Tudo por conta própria": autonomia individual e mediação técnica em aplicativos de autocuidado psicológico. **Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, v. 15, n. 1, p. 33-54, 2021. DOI: https://doi.org/10.29397/reciis.v15i1.2205. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2205/2415. Acesso em: 27 jun. 2022.

CUPPLES, Sarah. Frictionless design, frictionless racism. UX Collective. **Medium**, fev. 2021. Disponível em: https://uxdesign.cc/frictionless-racism-1097022d07f8. Acesso em: 27 jun. 2022.

DIETER, Michael; GERLITZ, Carolin; HELMOND, Anne *et al*. Multi-Situated App Studies: Methods and Propositions. **Social Media + Society**, v. 5, n. 2, p. 1-15, 2019. Disponível em: https://journals.sagepub.com/doi/10.1177/2056305119846486. Acesso em: 27 jun. 2022.

GOOGLE PLAY. **Cíngulo**: bem-estar mental. Disponível em: https://play.google.com/store/apps/details?id=com.cingulo.app&hl=pt_BR&gl=US. Acesso em: 27 jun. 2022.

KRUG, Steve. **Don't Make Me Think – Revisited**: A Common Sense Approach To Web Usability. 3. ed. Indianapolis: New Riders, 2005.

LARA, Diogo R.; BISOL, Luisa W.; BRUNSTEIN, Miriam G. *et al*. The Affective and Emotional Composite Temperament (AFECT) model and scale: a system-based integrative approach. **Journal of Affective Disorders**, v. 140, n. 1, p. 14-37, 2012. DOI: 10.1016/j.jad.2011.08.036. Disponível em: https://pubmed.ncbi.nlm.nih.gov/21978734/. Acesso em: 24 nov. 2021.

MAYER-SCHÖNBERGER, V.; CUKIER, K. **Big data**: A revolution that will transform how we live, work, and think. Boston: Houghton Mifflin Harcourt, 2013.

ROSE, Nikolas; ABI-RACHED, Joelle M. **Neuro**: The New Brain Sciences and the Management of the Mind. Princeton: Princeton University Press, 2013.

ROSE, Nikolas. **Governing the soul**: the shaping of the private self. Londres: Routledge, 1990.

ROSE, Nikolas. **Inventando nossos selfs**: psicologia, poder e subjetividade. Petrópolis: Vozes, 2011.

RUCKENSTEIN, Minna Susanna; DOW SCHÜLL, Natasha. The Datafication of Health. **Annual Review of Anthropology**, v. 46, out. 2017, p. 261-278. DOI: https://doi.org/10.1146/annurev-anthro-102116-041244. Disponível em: https://www.annualreviews.org/doi/abs/10.1146/annurev-anthro-102116-041244. Acesso em: 26 jun. 2022.

SAFATLE, Vladimir; SILVA JUNIOR, Nelson da; DUNKER, Christian. (Orgs.). **Neoliberalismo como gestão do sofrimento psíquico**. Belo Horizonte: Autêntica, 2020.

VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society**, v. 12, n. 2, p. 197-208, 2014. DOI: https://doi.org/10.24908/ss.v12i2.4776. Disponível em: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/datafication. Acesso em: 27 jun. 2022.

WHO. WORLD HEALTH ORGANIZATION. **Mental health and covid-19**. Copenhagen: WHO, mar. 2020. Disponível em: https://www.euro.who.int/en/health-topics/noncommunicable-diseases/mental-health/data-andresources/mental-health-and-covid-19. Acesso em: 14 maio 2020.

YOUNG, Victoria. Strategic UX: The art of reducing friction. **DTelepathy**, 2015. Disponível em: https://www.dtelepathy.com/blog/business/strategic-ux-the-art-of-reducing-friction. Acesso em: 14 jun. 2022.

https://doi.org/10.29397/EdicoesLivres/20250106

Marcada para morrer cedo: a história de Lorena e o impacto do uso indevido de dados de saúde na vida das pessoas

Giliate C. Coelho Neto

Num certo país, Augusto e Lorena são colegas de trabalho que demonstram interesse em contratar um seguro de vida. Empresas de seguros competem pelos clientes mais rentáveis – aqueles com melhores condições de saúde e maior expectativa de vida. O Open Health[23] está em pleno funcionamento e as empresas oferecem, inclusive, *cashbacks* para as pessoas que compartilham os seus dados de saúde, assim como descontos nos seguros, nos casos de comprovada higidez.

Augusto é um homem branco que está chegando próximo dos quarenta anos. Nenhum fato especial o motiva a adquirir o seguro – ele não possui doenças crônicas, faz atividades físicas regulares, goza de boa saúde mental, mora numa tranquila cidade e tem um bom emprego. Tem apenas um filho que mora com a ex-companheira e ele só o vê no fim de semana. Com o seguro, deseja apenas conferir uma segurança extra para a sua família, em caso de um inesperado sinistro.

A certeza quanto ao seu vigor físico e mental o motivam a autorizar a cessão de seus dados pessoais de saúde para as companhias de seguro, na expectativa de redução das mensalidades e de outros bônus. Tais dados incluem as anotações do seu médico em prontuário eletrônico, as doenças que já teve, os resultados de exames laboratoriais e de imagem, informações genéticas, o histórico das medicações consumidas, as internações e cirurgias às quais já foi submetido e as enfermidades dos familiares mais próximos.

Nos supercomputadores contratados pela seguradora escolhida, avançados algoritmos processam esses dados e os cruzam com outras informações da sua vida social: as faturas no supermercado, a quantidade de passos que dá por semana, quanto tempo permanece em média na academia e na tela do celular e

23 NE: Baseado no modelo do Open Bank, o Open Health é uma plataforma que tem dois pilares: a criação de um prontuário único dos pacientes que permita o compartilhamento de dados e o estímulo à concorrência na saúde suplementar por meio de maior agilidade na portabilidade. Segundo a Coalizão Direitos na Rede, o Open Health enfraquece o Sistema Único de Saúde (SUS) e viola os direitos dos pacientes, expondo-os à fragilidade na proteção de seus dados e à discriminação quanto ao acesso à saúde. Ver nota completa em: https://direitosnarede.org.br/2022/09/20/carta-aberta-os-perigos-do-open-health/

até seu histórico de tamanho das roupas compradas. A cessão de todos esses dados já havia sido previamente autorizada por Augusto sem ele saber, quando aceitou as letras miúdas das regras de compras nesses estabelecimentos.

O escrutínio das máquinas deixa claro: tratava-se de um exemplar raro de saúde naquela sociedade doente. Quarenta minutos de atividades físicas toda manhã, fartas feiras semanais com frutas, cereais, hortaliças e carnes magras, oito horas de sono por dia, dois livros lidos a cada mês. Nem mesmo o número da cintura havia aumentado nas últimas duas décadas. Toda essa saúde foi quantificada pelos algoritmos: expectativa de vida de 91 anos, risco de infarto ou derrame de menos de 0,1% nos próximos trinta anos e chance ínfima de desenvolver doenças crônicas como hipertensão e diabetes ao longo da vida.

Entram em cena, então, novos algoritmos que, baseados no perfil de consumo de Augusto, vão calcular quanto deve ser o desconto para que ele adquira imediatamente o seguro. É impulsivo diante de uma boa oferta? Costuma comparar preços antes de comprar algo? Gosta de negociar o valor? Estabelece *budgets*? Mais uma vez, as máquinas objetivam sua análise e estabelecem que, para fechar contrato imediato, o desconto precisa ser de, no mínimo, 50%. E assim é feito: Augusto está devidamente segurado.

Já sua amiga Lorena, mulher negra com um pouco mais de quarenta anos, não tem a mesma sorte. Augusto a convence a também tomar uma salvaguarda similar, argumentando ainda sobre as vantagens que obteve ao ceder seus dados. Colega no trabalho e lazer, ela também adere ao Open Health em busca de uma boa dedução no preço do seguro. Entretanto, para sua surpresa, além de não ter obtido o desconto, ainda lhe foi negada tal contratação. O que teria acontecido? Algum erro no cadastro da proposta? Uma análise equivocada por parte da Inteligência Artificial (IA)?

Buscando elucidar a situação, ela requisita uma revisão do seu pedido de seguro, dessa vez por um atendente humano, conforme prevê a legislação de seu país. O funcionário abre uma videochamada e pede um tempo para resgatar a ficha dela na empresa. Após alguns minutos, reabre a câmera e informa que o motivo para negação do pedido foi a baixa expectativa de vida atribuída a ela pelos algoritmos IA.

As máquinas a haviam dado uma expectativa de vida de 59 anos. O operador humano, todavia, não sabe explicar muito bem os motivos para isso. Como não? Pergunta ela, assustada. Que dados foram utilizados? Que critérios foram aplicados? Por que pessoas aparentemente similares conseguem contratar o seguro e eu não?

O operador explica que é impossível responder aos questionamentos. Com mais de três décadas de processamento de grandes volumes de dados e análise de milhões de pedidos, os supercomputadores, baseados em tecnologias de *Deep Learning*, iam aos poucos aperfeiçoando por si próprios seus algoritmos, de forma autônoma dos seus supervisores humanos. "É como se, depois de milhões de tentativas e erros com um número cada vez maior de dados de cada pessoa, as máquinas fossem aprendendo a acertar cada vez mais", diz o atendente, em explicação grosseira. E finaliza: "Isso não quer dizer que você viverá até os 57 anos... Você pode chegar aos noventa, cem anos... Às vezes esses computadores são conservadores demais em suas conclusões e..." Lorena agradece e encerra a videochamada, sem acreditar no que estava ouvindo. Num misto de emoções, sentia, de um lado, raiva da empresa por ter negado a ela um seguro, além do mal-estar por conta da frieza com que foi tratada, mas, por outro lado, era preenchida pela angústia do suposto diagnóstico da morte precoce.

Lorena é hipertensa e está um pouco acima do peso, mas toma seus remédios regularmente e faz atividades físicas. Haveria de ter um infarto? Um derrame? Sua pressão alta estava lhe fazendo um mal maior do que imaginava? Teria algum problema genético não diagnosticado? Ou um risco elevado de desenvolver um câncer? Mãe de dois filhos, atualmente com 38 anos, ela chega a fazer dezenas de exames, e ir a diversos especialistas, porém, nada descobre.

Insiste novamente junto à seguradora e pede uma nova análise que recusa a solicitação dela.

> – Não somos uma empresa de predição de expectativa de vida, diz um novo atendente num *chatbot*. Além disso, não temos como lhe dizer de forma precisa quais critérios foram utilizados pela nossa IA.
>
> – Como não? Vocês me deram trinta anos de vida a menos do que meu colega de trabalho, responde Lorena.
>
> – Essa projeção é destinada apenas ao cálculo de risco financeiro. A senhora pode viver 95, 110 anos...

Lorena percebe que o atendente é um *bot*, ou seja, um robô baseado em IA treinado para conversar com humanos. E, ao se lembrar de alguns trejeitos artificiais do funcionário, que a atendeu algumas semanas atrás, começa a desconfiar que também se tratava de um robô simulando um atendimento humano.

Ela pensa em acionar a empresa na Justiça, mas não tem nem tempo nem disposição para tal. Se resigna a conviver com a dúvida plantada pela IA sobre sua saúde, e reforçar o autocuidado e os exames preventivos.

Meses após esse episódio, ela recebe uma carta de seu banco informando a ela sobre um ajuste, para menos, em seus limites de crédito. Normalmente, não daria muita atenção a isso, mas como estava planejando financiar um apartamento, comparece a uma agência para entender melhor a mudança. Gentil, a funcionária explica que o banco tem contrato com uma empresa de dados especializada em projetar riscos futuros de clientes e que periodicamente atualiza seus limites de crédito baseado nas informações que recebe. Lorena permanece muda parecendo não acreditar no que ouve. Pede para ser informada sobre qual o prazo máximo de financiamento bancário ao qual teria direito. – Dez anos – responde a funcionária.

– Dez anos? Quem consegue comprar um apartamento em tempo tão curto?

Por um momento, chega a pensar em revelar a expectativa de vida que haviam dado anteriormente a ela, bem além do limite concedido pelo banco. Mas essa conversa era distópica demais para ela. Agradece à funcionária e se retira do banco. Segue catatônica pela cidade. Pega o metrô em direção à escola das filhas.

Após as crianças adormecerem, ela resolve pesquisar pela tal empresa de análise de dados na internet. Descobre que presta serviço a uma ampla gama de setores econômicos, inclusive seguradoras e entidades financeiras. Consegue descobrir a lista de clientes e lá estão a seguradora que recusou seu pedido e o seu banco. Tudo se encaixou... a empresa fez minuciosa análise dos seus dados e a compartilhou com seus outros contratantes.

Sente sua espinha gelar, quando vê que, na lista de clientes, também estão diversas empresas de recrutamento de recursos humanos. A madrugada vem e o sono não chega. Olha para as filhas, zanza pela casa, abre uma garrafa de vinho. Com a mente distante, vem uma estranha conclusão. É como se o ritual fúnebre de sua morte já tivesse sido iniciado. Marcada para morrer cedo, o sistema preventivamente ia se fechando, a expulsando aos poucos da vida. "Se perder meu emprego e não conseguir outro, é capaz de morrer até antes dos 59". Lorena se vê resignada, exausta e sem muitas forças para lutar contra algo que não sabe nem direito o que é. Vai em busca de descobrir que IA é essa que não permite revisão de seres humanos. Algumas buscas na internet e chega ao conceito de *Deep Learning*:

> Pelo *deep Learning*, o sistema passa a ser capaz não só de criar, mas também de estabelecer padrões de correlações próprias, desligados do raciocínio intelectual humano. (Pinto, 2020, p. 46)
>
> *Deep Learning* (aprendizagem profunda) é um ramo de *Machine Learning* usado para treinar computadores para realizar tarefas como seres humanos [...]. Um algoritmo de *Deep Learning* treina o computador para aprender sozinho através do reconhecimento de padrões em várias camadas de processamento. (Janos, 2022)
>
> A forma de treinar um algoritmo de *Deep Learning* é fornecer-lhe quantidades maciças de dados. Quantas mais análises ele fizer, mais preciso se torna. (Iberdrola, *s.d.*)

Lorena se vê muito preocupada. Essa sua forte preocupação é também vivenciada por diversos segmentos da sociedade, desde duas décadas atrás, quando a crescente dificuldade em se revisar decisões tomadas com base em IA começam a fazer parte da nossa sociedade:

> As decisões têm sofrido um intenso processo de automatização baseada em critérios na maioria das vezes não conhecidos ou bem explicados por seus criadores, de modo que passam a ter grande influência no dia a dia das pessoas sem que elas necessariamente percebam. (Pinto, 2020, p. 50)

Lorena descobre que os primórdios do seu problema começaram no início do século XXI, quando seguradoras de vida passam a utilizar dados pessoais de saúde para oferecer descontos nos seus serviços. Surgem também empresas especializadas em projetar riscos de morte, baseados nesses dados. Os dados eram obtidos a partir de questionários, prontuários eletrônicos, bancos de dados farmacêuticos, contas em redes sociais, entre outros. Caso o cliente optasse por não ceder seus dados de saúde, teria que pagar um seguro mais caro (Moyet, 2022).

Planos e seguradoras de saúde seguiram pelo mesmo caminho, utilizando análises avançadas sobre grandes bases de dados para projetar custos dos usuários e modelar suas ofertas assistenciais. Apesar de diversos países, incluindo o Brasil, em período anterior, proibirem a negativa de contratação de um seguro-saúde devido a uma doença preexistente, o uso de dados pessoais podia ser utilizado indevidamente para restringir ou dificultar certos tipos de procedimentos (Allen, 2018).

Ela fica surpresa ao ver que as primeiras empresas especializadas em análises e projeção de riscos em saúde já utilizavam uma ampla gama de dados da população.

Recortou um trecho específico de uma matéria, encontrada em um *site* desativado, sobre uma empresa chamada LexisNexis, no qual era afirmado que:

> [...] usa 442 atributos pessoais não médicos para prever os custos médicos de uma pessoa. Seu cachê inclui mais de 78 bilhões de registros de mais de 10.000 fontes públicas e proprietárias, incluindo números de celular de pessoas, registros criminais, falências, registros de propriedade, segurança do bairro e muito mais. As informações são usadas para prever os riscos e custos de saúde dos pacientes em oito áreas, incluindo a frequência com que eles visitam as salas de emergência, seu custo total, seus custos de farmácia, sua motivação para se manter saudável e seus níveis de estresse. (Allen, 2018)

Perto do dia amanhecer, Lorena ainda adentra em mais arquivos antigos da internet e descobre que foram realizadas várias tentativas de se efetivar um controle público sobre as avançadas tecnologias de IA que passaram a ser utilizadas em massa por empresas e governos. Toma um susto ao ler uma reportagem escrita anos atrás:

> É um faroeste lá fora para a Inteligência Artificial. Os aplicativos de IA são cada vez mais usados para tomar decisões importantes sobre a vida dos humanos com pouca ou nenhuma supervisão ou responsabilidade. Isso pode ter consequências devastadoras: prisões injustas, notas incorretas para os alunos e até ruína financeira. Mulheres, grupos marginalizados e pessoas de cor geralmente carregam o peso da propensão da IA ao erro e ao exagero. (Heikkilä, 2022)

Seria ela uma dessas vítimas da IA? Ela encara a dúvida com indignação, mas também com uma certa esperança. Talvez o veredicto sobre a expectativa de vida tenha sido influenciado por alguma análise enviesada das máquinas.

Outros diversos documentos que ela encontra mostram a importância do debate ético sobre a IA e o imperativo de intervenção humana toda vez que isso se mostra necessário:

> Os sistemas de IA devem ser projetados de maneira a respeitar o Estado de Direito, os direitos humanos, os valores democráticos e a diversidade, liberdade, dignidade, autonomia, privacidade e proteção de dados, não discriminação e igualdade, diversidade, equidade, justiça social e direitos trabalhistas internacionalmente

> reconhecidos. Para isso, devem incluir salvaguardas apropriadas, como possibilitar a intervenção humana sempre que necessário. (Hartmann *et al.*, 2020, p. 6)

Ela percebe que uma das razões para a derrota das tentativas de regular a IA estava relacionada ao poder das grandes empresas de tecnologia, que alegavam burocracia excessiva e abertura do sigilo empresarial para auditores externos. Algumas das matérias que encontrou diziam: "Uma crítica comum dos lobistas do Vale do Silício é que o regulamento criará burocracia extra para as empresas de IA" (Heikkilä, 2022). E a matéria ainda completava que: "As empresas de tecnologia também estão profundamente desconfortáveis com os requisitos para dar aos auditores ou reguladores externos acesso ao seu código-fonte e algoritmos para fazer cumprir a lei" (Heikkilä, 2022).

Mas ela também nota que não foi possível desenvolver ferramentas adequadas para auditar de forma satisfatória os algoritmos da IA, que se desenvolveram num ritmo muito mais veloz do que as tecnologias elaboradas pelos governos e pelas entidades da sociedade civil. A aposta excessiva na revisão humana sobre as decisões das máquinas também foi outro erro. Se todos reconheciam, já naquela época, a autonomia e a velocidade do aprendizado das máquinas, como imaginaram que um pobre grupo de seres humanos teria capacidade de reavaliar a contento milhares de análises e de decisões supostamente equivocadas?

O que ela encontra de mais promissor, que talvez a pudesse ter protegido das exclusões sofridas, é uma proposta de simplesmente proibir que decisões sobre a vida das pessoas possam ser baseadas em IA. Numa espécie de museu virtual da internet, ela encontra uma proposta de classificação "risco de IA" baseada em quatro níveis: inaceitável, alto, limitado ou mínimo (European Commission, 2021)[24].

O primeiro era enfático: "Todos os sistemas de IA considerados uma clara ameaça à segurança, aos meios de subsistência e aos direitos das pessoas serão banidos". Já no risco considerado alto, estavam as tecnologias de IA utilizadas em:

> [...] emprego, gestão de trabalhadores e acesso ao autoemprego (por exemplo, *software* de triagem de currículo para procedimentos de recrutamento).
>
> [...] serviços públicos e privados essenciais (por exemplo, pontuação de crédito que nega aos cidadãos a oportunidade de obter um empréstimo). (European Commission, 2021)

24 Tradução do autor.

Essas tecnologias não seriam a princípio banidas, mas objeto de intenso controle por órgãos reguladores, que deveriam registrar as suas atividades de forma a garantir a rastreabilidade dos resultados e elaborar uma documentação detalhada com todas as informações necessárias para auditorias e avaliações de conformidade. "Será que foi aí que a coisa não deu certo?", pensa ela.

O dia amanhece e logo as meninas vão acordar para mais um dia na escola. Chove torrencialmente na cidade e ela já prevê a dificuldade em levá-las à escola por conta do transporte público, mas não há outra opção. Não pode se dar ao luxo de faltar ao trabalho para cuidar delas, principalmente depois de tudo que viu. Larga o celular e corre para preparar o café da manhã.

Referências

ALLEN, Marshall. Health Insurers Are Vacuuming Up Details About You – And It Could Raise Your Rates. **ProPublica**. 17 jul. 2018. Disponível em: https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates. Acesso em: 10 jan. 2024.

EUROPEAN Commission. Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future [Internet]. 2021 [cited 2022 Jul 4]. Available from: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

HARTMANN, I. A.; FRANQUEIRA, B.; IUNES, J.; ABBAS, L.; CURZI, Y.; VILLA, B. *et al.* Policy Paper: Regulação de Inteligência Artificial no Brasil. **FGV Direito Rio**. 2020. Disponível em: https://direitorio.fgv.br/conhecimento/policy-paper-regulacao-de-inteligencia-artificial-no-brasil. Acesso em: 10 jan. 2024.

HEIKKILÄ, Melissa. A quick guide to the most important AI law you've never heard of. **MIT Technology Review**. 13 maio 2022 Disponível em: https://www.technologyreview.com/2022/05/13/1052223/guide-ai-act-europe/?utm_campaign=site_visitor.unpaid.engagement&utm_medium=tr_social&utm_source=Twitter. Acesso em: 10 jan. 2024.

IBERDROLA. "Deep learning": um conceito-chave para levar a Inteligência Artificial a um nível superior. *s.d.* Disponível em: https://www.iberdrola.com/inovacao/deep-learning. Acesso em: 10 jan. 2024.

JANOS, Michel. Deep Learning – Conceitos e aplicações. 2022. Disponível em: https://www.3dimensoes.com.br/post/deep-learning-conceitos-e-aplicações. Acesso em: 09 nov. 2023.

MOYET, Paolo. How Life Insurance Companies Get Intel On You. Forbes. 9 jun. 2022. Disponível em: https://medium.com/@jrpmoyet/how-life-insurance-companies-get-intel-on-you-b8de4ea85a3e. Acesso em: 15 fev. 2024.

PINTO, H. A. A utilização da Inteligência Artificial no processo de tomada de decisões: por uma necessária accountability. **Revista de Informação Legislativa**, v. 57, n. 225, jan.-mar. 2020, p. 43-60. Disponível em: https://www12.senado.leg.br/ril/edicoes/57/225/ril_v57_n225_p43. Acesso em: 20 jan. 2024.

https://doi.org/10.29397/EdicoesLivres/20250107

Compartilhamento de dados e saúde suplementar: limites e possibilidades do Open Health

Bárbara Simão

Em março de 2022, o então ministro da saúde do Brasil, Marcelo Queiroga, afirmou que a implementação do Open Health no país seria questão de "tempo, coragem e decisão" (Queiroga, 2022). A possibilidade desse novo modelo para o compartilhamento de dados entre empresas operadoras de saúde tem sido aventada desde janeiro de 2022, na esteira das discussões sobre um sistema parecido aplicado para o setor financeiro – o Open Banking. O sistema teria o objetivo de criar um registro nacional de dados sobre pacientes e indicadores sobre saúde suplementar a ser compartilhado entre operadoras e pacientes. A possibilidade também entra no escopo de uma série de mudanças introduzidas no panorama da saúde com a evolução de novas tecnologias e de suas capacidades de análise e compartilhamento de dados.

Essa é uma questão que veio para permanecer. Especialmente a partir da pandemia de covid-19, as intersecções possíveis entre saúde e tecnologia têm se alargado mundo afora. No Brasil, isso se revela a partir da regulamentação da telemedicina, por exemplo, que veio a cabo em maio de 2022 (Felix, 2022). Nessa esteira, também ganham atenção as possibilidades de uso de dados da população para aplicações de saúde.

Tais inovações, no entanto, incorrem em implicações relevantes ao direito à privacidade e à proteção de dados dos cidadãos, que merecem ser avaliadas previamente à implementação de um sistema como o Open Health. O uso de informações de saúde pode revelar padrões significativos, entre doenças, hábitos de vida e até perfil genético. Analisadas em conjunto, há expressivas possibilidades de danos, de serem utilizadas de maneira discriminatória ou, ainda, de incidentes de segurança com as informações armazenadas. Não à toa, a Lei Geral de Proteção de Dados Pessoais (LGPD) considera informações sobre saúde como "dados sensíveis", sujeitos a maior grau de proteção jurídica. Desse ponto, deriva também o questionamento a respeito da compatibilidade desse sistema com a legislação

hoje existente no país. Seria possível sua aplicação, hoje, no Brasil? Haveria limites legais para tanto?

Assim, partindo desse caso, este capítulo terá como objetivo compreender as bases e origens da ideia de Open Health, bem como suas possíveis aplicações e limites. Para tanto, o artigo irá abordar as origens e inspirações para o sistema, apoiando-se brevemente sobre o conceito de "financeirização" (Krippner, 2017) e de "financeirização digital" (Jain; Gabor, 2020) de forma a compreender como a relação imbricada entre as empresas de tecnologia e as do setor financeiro pode jogar luz sobre um processo que abrange também o setor da saúde, em especial, a saúde suplementar. Se a separação entre a vida digital e a vida financeira torna-se cada vez mais difícil, a partir da criação de um espaço híbrido entre ambos, nos quais dados são o ingrediente crítico para novas possibilidades de geração de lucro e governança (Jain; Gabor, 2020, p. 818), esse hibridismo também é vislumbrado para o setor de saúde. Assim, a partir de um paralelo da ideia de Open Health com as experiências no setor financeiro e com a regulação do Open Banking, este texto busca explorar as diferentes premissas e possibilidades de cada sistema.

Por fim, o capítulo também se propõe a avaliar como um sistema de Open Health poderia se compatibilizar (ou não) com o arcabouço normativo sobre proteção de dados no país. Isto é, quais as limitações legais e regulatórias hoje existentes para uma política como essa?

1. Entre finanças, saúde e tecnologia

O Open Health é um sistema que intersecciona finanças, saúde e tecnologia, criando um espaço híbrido entre essas diferentes esferas. Entender o contexto de implementação de um sistema como esse pode ser relevante para, também, entender seus possíveis desenvolvimentos futuros. Nesse sentido, vale comentar como o papel crescente das finanças na economia e no acesso a diferentes tipos de bens e serviços tem sido objeto da literatura já há algum tempo. Analisa-se como instituições financeiras ganharam centralidade, especialmente a partir da década de 1970, no provimento de "bem-estar" à população. Esse fenômeno faz parte do que alguns autores chamam de "financeirização" da economia. Embora haja divergência sobre quais seriam os seus significados[25], e, inclusive, sobre a pertinência atual do conceito (Christophers, 2015), pode-se afirmar que uma definição abrangente descreveria a financeirização como o "papel crescente de motivos financeiros, mercados financeiros, atores financeiros e instituições

25 Algumas definições são sistematizadas por Greta Krippner no 2º capítulo de seu livro. Cf. (Krippner, 2011).

financeiras na operação das economias doméstica e internacional" (Epstein, 2005, p. 3). Da mesma maneira, há certo consenso de que esse processo se refletiu em uma alteração das relações de crédito, que passaram a adquirir um papel central na economia como forma de sustento para o consumo (Sawyer, 2013, p. 3; Lavinas; Araújo; Bruno, 2017, p. 6).

O acesso ao crédito ganha, assim, peso de garantia de provimento social à população (Atkinson, 2019). De acordo com Lena Lavinas, benefícios sociais passam, por meio desse processo, a ser ligados ao crédito, que então ganharia protagonismo no provimento de saúde, seguridade social, educação e bem-estar da população, de maneira geral. Esse movimento faria com que, para grande parcela da população, mais valesse a contratação de um plano de saúde ou de uma escola privada que a utilização do serviço público (Lavinas, 2017, p. 176). A esfera de proteção social dos cidadãos, assim, ficaria intermediada pelas finanças e pelo endividamento da própria população, em lugar do Estado (Crouch, 2009, p. 390).

Uma das críticas ao conceito de financeirização reside no fato de que ele seria amplo demais e, dada a amplitude, incapaz de descrever precisamente determinados fenômenos (Christophers, 2015). Porém, no caso em análise, ele interessa menos por sua capacidade de oferecer explicações a um fenômeno específico, e mais como suporte para o contexto em que se destacam iniciativas que integram finanças à perspectiva de proteção social de cidadãos – sem deixar de considerar que, atualmente, a tecnologia agrega novas nuances a esse debate.

Jain e Gabor (2020) cunharam a expressão "financeirização digital" pensando nas relações imbricadas que abrangem o setor financeiro e a tecnologia. De acordo com os autores, esse processo envolveria a criação de uma esfera híbrida – entre a tecnologia e as finanças – que permitiria novas possibilidades de lucro, a partir da vigilância de indivíduos. Os autores se amparam na noção de "capitalismo de vigilância", desenvolvida por Shoshana Zuboff, o qual seria o "modelo padrão do capitalismo de informação na internet" e se organizaria em torno da extração de dados pessoais sobre comportamento de indivíduos (Zuboff, 2019, p. 152). Dados pessoais, segundo a autora, seriam a matéria-prima desse modelo de negócios: quanto maior a extração de dados, maior seria o potencial de exatidão dos produtos de predição resultantes de sua análise.

Partindo dessa percepção, Jain e Gabor afirmam que a financeirização digital envolveria o uso de dados, enquanto ingrediente crítico para a obtenção de lucro por empresas do ramo da tecnologia e finanças. O lucro não estaria na receita proveniente de pagamentos, mas no uso de dados colhidos e monetizados, visando à criação de perfis mais detalhados de clientes para venda de produtos.

O motor seria a crescente inovação em torno de infraestruturas digitais promovida por empresas de tecnologia e *fintechs*, com apoio de políticas governamentais de digitalização da economia.

A análise dos autores, no entanto, encerra-se na integração entre tecnologia, finanças e acesso ao crédito, não abordando a integração desse fenômeno com outros setores específicos – como, por exemplo, acesso à saúde. O caso do Open Health¸ por sua vez, chama atenção justamente pelo fato de que a integração entre a esfera financeira e a tecnológica se alia também às possibilidades de uso de dados em saúde. Nesse caso, a vigilância não ocorreria unicamente sobre informações financeiras, mas também sobre o conteúdo de informações sanitárias da população – o que abriria margem para diferentes tipos de extração de dados e ferramentas preditivas.

O hibridismo entre as esferas financeira e tecnológica, assim, alcança esses novos campos, diante das novas possibilidades apresentadas para geração de lucro. Isso se vislumbra também no crescimento do setor das *healthtechs*, *startups* de inovação em saúde que, entre 2018 e 2020, cresceram 118% no Brasil (Carmen, 2021). Inovações tecnológicas para o setor de saúde estão em crescimento e vão desde a criação de plataformas de intermediação para consultas e exames até ferramentas de utilização de Inteligência Artificial (IA) para auxílio em diagnósticos (Chakraborty; Ilavarasan, 2021).

É nesse contexto que se insere a ideia de Open Health. Mesmo que embrionário, o plano do governo anuncia o interesse em um modelo de negócios que tende a permanecer. Assim, nos próximos tópicos, iremos entender quais foram as origens e inspirações para um projeto como esse, bem como os seus limites de aplicação no âmbito da legislação brasileira.

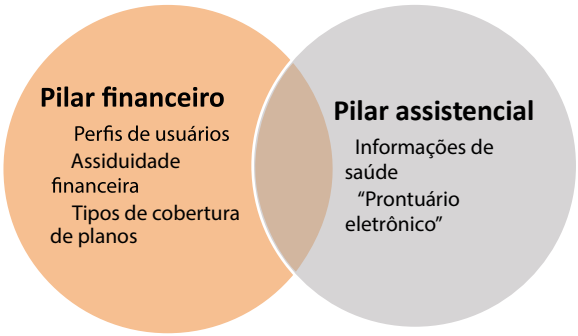
2. O Open Health e as suas inspirações

De acordo com o ministro da Saúde, quando anunciou a possibilidade da medida, o Open Health seria formado por dois pilares: um financeiro e outro assistencial. O pilar assistencial serviria como um repositório de dados de saúde dos brasileiros, formado a partir da Rede Nacional de Dados em Saúde (RNDS). O sistema funcionaria como um "prontuário eletrônico", em que todas as informações relevantes referentes à saúde de uma pessoa ficariam ali, armazenadas, para compartilhamento, conforme a necessidade.

O pilar financeiro, conforme afirmou Queiroga (2022), seria como um "cadastro positivo" para a saúde. Perfis de usuários, assiduidade financeira e tipos de

cobertura de planos de saúde poderiam ficar visíveis às operadoras. A intenção, com isso, seria de facilitar a portabilidade de informações entre empresas.[26]

Figura 1 – Pilares do Open Health, de acordo com o ministro da Saúde



Fonte: Elaborada pela autora (2024).

A ideia de Open Health vislumbrada pelo governo brasileiro difere-se, assim, de uma perspectiva de acesso à informação ou de dados abertos governamentais (*open data* ou *open government data*). Nesses casos, o intuito é alavancar a transparência das ações do Estado, por meio de abertura de bancos de dados produzidos por agências governamentais e referentes às políticas públicas ou ações do governo sobre determinada questão, incentivando o escrutínio público (Heijlen; Crompvoets, 2021). A abertura de dados, no caso do Open Health, não seria feita ao público ou com o intuito de incrementar a transparência estatal, mas no sentido de criar uma plataforma de incentivo à interoperabilidade e ao compartilhamento de dados entre diferentes instituições pertencentes ao setor da saúde.

Há pouca literatura produzida a respeito dessa categoria de Open Health, até onde foi possível acessar em um primeiro levantamento. A maioria dos artigos produzidos a respeito aborda o tema a partir da perspectiva do *open data*, seja identificando limites e possibilidades no compartilhamento de dados de saúde pelo governo[27], seja por meio de estudos de caso de sistemas de dados abertos em saúde.[28] É possível, no entanto, identificar de onde vieram algumas das inspirações para o modelo

26 Hoje, a Agência Nacional de Saúde Suplementar (ANS) prevê regras de portabilidade de carências entre planos de saúde, isto é, a possibilidade de trocar de plano sem necessidade de cumprir carência ou cobertura parcial temporária. O direito está previsto na Lei dos Planos de Saúde (lei n. 9.656/1998). Não há, todavia, regra a respeito da portabilidade de dados na saúde suplementar.

27 Nesse sentido: HEIJLEN, Roel; CROMPVOETS, Joep. Open Health Data: Mapping the ecosystem. **Digital Health**, 2021. D'AGOSTINO, Marcelo; MARTI, Myrna; MEJÍA, Felipe; DE COSIO, Gerardo; FABA, Gladys. Estrategia para la gobernanza de datos abiertos de salud: un cambio de paradigma en los sistemas de informacion. **Revista Panamericana de Salud Pública**, 2017.

28 Nesse sentido: BULLINGER, Angelika C., et. al. Open innovation in Health Care: analysis of an Open Health Platform. **Health Policy**, Amsterdam, v. 105, n. 2-3, 2012, p. 165-175. BEGANY, Grace M.; MARTIN, Erika G. An Open Health Data engagement ecosystem model: are facilitators the key to open data success? Proceedings of the Association for Information Science and Technology, v. 54, n. 1, out. 2017, p. 621-623.

vislumbrado e, a partir daí, traçar alguns paralelos. Nas próximas seções, portanto, veremos duas delas: o Open Banking, sistema que tem avançado na regulação financeira de diferentes jurisdições e já foi implementado pelo governo brasileiro, e a National Digital Health Mission (NDHM), implementada nos últimos anos pelo governo da Índia.

2.1 O Sistema Financeiro Aberto (Open Banking) e a sua regulamentação pelo Banco Central

Uma das inspirações expressas para o Open Health seria o Open Banking (Sistema Financeiro Aberto), modelo aplicado ao setor financeiro e regulamentado pelo Banco Central do Brasil (BCB), a partir do ano de 2020. O Open Banking é uma tendência na regulação financeira em diversas jurisdições (Zachariadis; Ozcan, 2017). Por meio do modelo, busca-se o "compartilhamento padronizado de dados e serviços por meio de abertura e integração de plataformas e infraestruturas de sistemas de informação" por instituições do setor financeiro (Banco Central do Brasil, 2019). Isto é, pretendeu-se criar uma interface entre diferentes instituições que facilitasse o compartilhamento de informações financeiras de indivíduos. A vantagem do sistema, de acordo com o Banco Central, seria incentivar a maior concorrência entre empresas do setor financeiro, uma vez que o indivíduo teria maior liberdade e controle para definir com quais instituições poderia solicitar o compartilhamento de uma informação ou não.[29]

A proposta de regulamentação do Open Banking passou por rodadas de discussão e consulta pública, da qual participaram empresas do ramo financeiro, pessoas físicas e entidades da sociedade civil (Banco Central do Brasil, 2019). Por fim, o órgão chegou à resolução conjunta n. 1/2020, que dispõe sobre a implementação do sistema e os seus requisitos de operação.

No escopo do Open Banking, há a instituição detentora de dados (aquela que compartilha) e a instituição receptora de dados (aquela que recebe o dado compartilhado). O consentimento do titular dos dados é a base para a operação do sistema – é o cliente quem define quando, como e com quem suas informações poderão ser compartilhadas.

Conforme o art. 10 da resolução, a instituição receptora deve obter o consentimento do cliente de maneira informada, atendo-se a finalidades predeterminadas, por prazo de validade compatível a essas finalidades e limitado a 12 meses, discriminando os dados e serviços que serão objeto de compartilhamento entre

29 Disponível em: https://openbankingbrasil.org.br/conheca-o-open-banking/. Acesso em: 5 set. 2022.

as instituições. Também é vedada a manifestação do consentimento por meio de contrato de adesão ou de forma presumida, sem manifestação ativa do cliente. Além disso, há diversos requisitos de segurança da informação previstos pela normativa e por outras circulares e resoluções do Banco Central a esse respeito.

As normativas do BCB também previram uma estrutura de governança responsável por acompanhar a implementação do sistema. De acordo com a circular n. 4.032/2020, a estrutura seria composta por três níveis: Conselho Deliberativo, responsável por decidir as questões estratégicas necessárias para a implementação do projeto no país e propor os padrões técnicos ao Banco Central; Grupos Técnicos, responsáveis por desenvolver estudos, propostas técnicas e planos de trabalho; e Secretariado, responsável por organizar os planos de trabalho e as propostas técnicas apresentadas. O Conselho seria composto por sete representantes, entre os quais seis seriam indicados por associações ou grupos de associações com representação significativa de instituições autorizadas a funcionar pelo Banco Central, e um "conselheiro independente", sem vínculo com instituição participante do Open Banking, com desempenho de suas funções em "favor da competição, da inovação, da segurança e privacidade de dados, bem como da proteção do consumidor" (art. 9º, §1º, circular n. 4.032/2020).

Atualmente, prevê-se a expansão do sistema para abarcar não apenas produtos bancários, mas também serviços financeiros como câmbio, seguros e previdência. Por essa razão, o BCB alterou a nomenclatura da resolução conjunta de Open Banking para Open Finance, buscando maior amplitude em sua significação (G1, 2022).

Assim, pode-se dizer que o sistema financeiro aberto apresenta robusta estrutura regulatória e de governança, sendo regido por diferentes especificações normativas e técnicas colocadas pelo Banco Central. Tal ponto é de suma importância considerando-se a magnitude do sistema e o seu impacto sobre dados pessoais de cidadãos. Vale dizer, ainda, que os fluxos de informação no âmbito financeiro são bastante diferentes daqueles existentes no setor de saúde. A aplicação de um sistema para um setor, assim, não necessariamente significa que funcionaria para outro, considerando-se todas as particularidades pertinentes ao uso e ao tratamento de informações de saúde.

2.2 O Open Health indiano

Mirando fora do contexto nacional, a Índia também serviu de inspiração para o modelo do Open Health. Há, no país, um sistema de formatação em moldes semelhantes, implementado a partir de 2020. Trata-se da National Digital Health

Mission (NDHM), a partir da qual é gerada uma identidade nacional de saúde para cada cidadão, a qual agrega suas informações de saúde (Shrivastava, 2021). A identidade digital de saúde pode ser criada por meio de registro eletrônico *on-line*, de aplicativo no celular ou de visita aos centros de saúde comunitários ou hospitais. Ela pode ser criada a partir do número de identidade civil da Índia, o Aadhaar.[30]

A identidade digital da NDHM serviria para a implementação de um registro pessoal de saúde, o qual conteria todas as informações relacionadas à saúde desse indivíduo, bem como um registro médico que contivesse todo o histórico médico e de tratamento de um paciente. Esse registro conteria informações sobre todos os exames, doenças, médicos visitados, prognósticos e medicações. A ideia, assim, seria de algo próximo a um grande repositório de prontuários eletrônicos de um mesmo paciente, que agregasse todo o seu histórico médico e as suas condições de saúde em um local. Algo semelhante, assim, ao que propõe o ministro Marcelo Queiroga, no caso brasileiro.

Críticas têm sido feitas ao projeto indiano em diversas direções. Além das questões relacionadas aos possíveis impactos sobre a privacidade de cidadãos, uma delas contesta a NDHM no sentido de que ela seria mais um incentivo ao setor privado do que algo que levaria em conta interesses de saúde pública ou benefícios concretos aos cidadãos (Aravindakshan, 2021). A justificativa de revolução da saúde por meio de soluções tecnológicas não se sustentaria na prática, e o acesso às grandes quantidades de dados de cidadãos seria, na verdade, um chamariz para que as empresas de saúde suplementar investissem no mercado (Aravindakshan, 2021).

Questiona-se, ademais, o quanto a ausência de uma identidade de saúde digital poderia levar à exclusão de cidadãos do próprio sistema de saúde, ou sua adesão compulsória ao sistema (Aravindakshan, 2021). Seria o caso, por exemplo, de dificuldades no acesso às vacinas ou ao atendimento médico, em virtude da ausência do número de identidade de saúde. De outro lado, também foi relatado que, no âmbito da vacinação da covid-19, a identidade de saúde acabou sendo atribuída automaticamente às pessoas que optaram pela identificação pelo registro civil Aadhaar (Shrivastava, 2021).

Sendo assim, o caso indiano, mais próximo ao que o governo brasileiro pretende implementar, no âmbito da saúde, evidencia como o assunto merece reservas. O Open Banking, por outro lado, mostra a necessidade de que o tema seja

30 O Aadhaar é o número de identidade digital única da Índia, composto por 12 dígitos e ligado a informações biométricas como impressão de digitais, íris e fotografia da face. Cf. RAO, Ursula; NAIR, Vijayanka. Aadhaar: Governing with Biometrics. **South Asia: Journal of South Asian Studies**, v. 42, n. 3, 2019, p. 469-481.

profundamente discutido, antes de qualquer tentativa de implementação, bem como a necessidade de normativas e de um sistema de governança e fiscalização regulatória criterioso. Diante dessas dificuldades, seria possível termos algo próximo a um sistema de Open Health no Brasil? Ou, ainda, esse sistema seria compatível com a legislação brasileira sobre proteção de dados? Tais questões, então, serão objeto de análise na próxima seção, em que a premissa geral do sistema será colocada em questionamento diante da LGPD.

3. O Open Health e a Lei Geral de Proteção de Dados Pessoais (LGPD): aproximações e dissonâncias

Retomando a ideia do sistema anunciado pelo governo brasileiro, temos a premissa do sistema calcada em dois pilares: um assistencial, referente a uma espécie de registro de prontuário eletrônico vitalício; e um financeiro, referente ao que poderia ser uma espécie de plataforma para troca de informações entre operadoras – algo que o ministro Marcelo Queiroga batizou de "cadastro positivo" das operadoras de saúde.

3.1 O pilar financeiro: é possível falar de um "cadastro positivo da saúde"?

De início, o projeto de um cadastro positivo da saúde merece atenção. O tema vai além da portabilidade de dados. Em linhas gerais, a ideia por trás da pontuação de crédito e do cadastro positivo, regulamentado pela lei n. 12.414/2011, é discriminar pessoas de acordo com suas capacidades de pagamento: caso sejam lidas como "boas pagadoras" por algoritmos de predição formulados por birôs de crédito, terão uma nota mais alta, o que implica melhores condições de juros para aquisição de empréstimos, financiamentos, compras a prazo, entre outras possibilidades.

Uma vez que a relação de crédito é permeada por assimetrias de informação, o sistema baseia-se na premissa de que um ambiente com maiores informações sobre indivíduos geraria menos efeitos de seleção adversa na economia – e, consequentemente, juros mais baixos (Stiglitz, 1981). Assim, o intuito desses sistemas é ser um mecanismo de triagem capaz de "mensurar" as incertezas inerentes às operações de crédito, transformando-as em uma determinada classificação e quantidade de risco "calculável" que uma pessoa ou empresa oferece (Carruthers, 2015). Faz-se a análise sobre diferentes informações apresentadas por aquele consumidor e estima-se uma nota para ele. Essa nota, por sua vez, é baseada em análises estatísticas que apresentem correlações entre determinados comportamentos e adimplemento de obrigações.

A implementação do cadastro positivo, no entanto, não surgiu livre de críticas. Sistemas de avaliação de risco de crédito têm sido questionados desde meados do século XX, nos EUA, dados os impactos possíveis sobre a privacidade de cidadãos e as possibilidades de discriminação no acesso ao crédito (Matheson, 1984). O processamento automatizado de dados com a expansão de sistemas algorítmicos capazes de analisar volumes massivos de informação ainda agrega nuances a esse debate.

Citando, brevemente, três conjuntos de problemas, podem ser elencados: (i) a possibilidade de reprodução de vieses discriminatórios ou o reforço de desigualdades previamente existentes na análise feita por algoritmos (Charron-Chénier; Seamster, 2021; Eubanks, 2017; Noble, 2018); (ii) a transparência no uso de informações, considerando-se a complexidade de se traduzir como um algoritmo pode tomar uma decisão (Pasquale, 2015); e (iii) a dificuldade de acesso à reparação ou à correção em caso de eventuais injustiças (Matheson, 1984).

Dados os impactos do sistema sobre a privacidade de cidadãos, o cadastro positivo passou por debates no Legislativo que se estenderam por mais de dez anos até que uma lei sobre o assunto fosse aprovada e, ainda hoje, o tema é objeto de discussões.[31]

Transferir essa lógica para a saúde suplementar poderia significar não apenas uma facilidade de portabilidade entre empresas, mas também uma lógica de discriminação, a partir das informações sobre a saúde de um indivíduo. É nesse ponto que mora o problema: caso haja acesso às informações sobre saúde de um indivíduo, uma operadora de saúde poderia cobrar mais caro pelo serviço ou por uma mensalidade personalizada que refletisse as condições e os hábitos de vida daquele sujeito. Por exemplo, caso uma operadora de saúde analisasse que uma pessoa tem hábitos de vida que geram "maior risco" à sua saúde. A depender da análise estatística feita, isso poderia significar avaliar negativamente uma pessoa por problemas de saúde mental, por seus hábitos alimentares, e até por outras questões não diretamente relacionadas à saúde do indivíduo em si, mas às suas condições ambientais, como local de residência. As possibilidades de criação de perfis e de discriminação a partir disso são inúmeras.

É desse modo que falar em "cadastro positivo da saúde" gera estranhamento, já que, a princípio, não pareceria haver qualquer benefício ao consumidor final, mas uma personalização de preços, a partir de suas informações pessoais. No mais, toda a ideia de controle exercido pelo consumidor também perde sentido, já que um dos

31 A Lei do Cadastro Positivo ainda passou por revisão, em 2019. Uma das principais mudanças na alteração legislativa foi o fim da exigência de consentimento de cidadãos para que suas informações passassem a ser compartilhadas entre instituições financeiras e birôs de crédito.

pontos mais criticados em relação ao cadastro positivo é a falta de transparência quanto aos critérios dos sistemas que fazem a avaliação de risco.

Se em abstrato a ideia já merece reservas, quando observadas as disposições da LGPD, fica evidente o intuito legislativo de se evitar que práticas como essa ocorressem. Na LGPD (Art. 11, II), há algumas bases legais e especificações que se relacionam ao uso de informações de saúde. São elas: "[...] 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".

Enquanto a primeira base legal relaciona-se a situações mais emergenciais que coloquem a vida de pessoas em risco e que, portanto, justifiquem a necessidade do tratamento de dados, a segunda é aquela utilizada para procedimentos de saúde em geral. Há, no entanto, importante especificação relacionada ao uso de informações de saúde com objetivo de obter vantagem econômica:

> § 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 à 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.
>
> § 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. (LGPD, grifos da autora)

A partir da leitura dos parágrafos em conjunto, é possível abstrair (i) uma vedação geral à obtenção de vantagem econômica por meio de compartilhamento de informações de saúde, excetuados determinados casos de prestação de serviço, portabilidade de dados e transações financeiras e administrativas, bem como (ii) uma vedação à prática de seleção de riscos, na contratação de modalidades de planos privados de assistência à saúde.

Assim, qualquer tipo de precificação de planos com base em informações de saúde fica expressamente vedada pela legislação. A ideia de um "cadastro positivo da saúde", portanto, não se sustenta em termos jurídicos, uma vez que houve cuidado em se evitar a prática de seleção de riscos nessa área.

Uma iniciativa como essa só seria possível caso qualquer possibilidade de avaliar riscos com base nos dados pessoais de saúde dos indivíduos estivesse fora de cogitação. Isso apenas seria possível caso houvesse uma separação completa de sistemas, estrutura e governança entre a vertente assistencial e a vertente financeira do sistema do Open Health. Isto é, ambas as vertentes não poderiam se comunicar de maneira alguma, já que qualquer mínima possibilidade de integração entre ambas (entre sistemas) esbarraria nas vedações previstas pela LGPD. Diante dessa impossibilidade, questiona-se até que ponto se sustentaria a viabilidade de um pilar financeiro para o Open Health, uma vez que ele, por princípio, teria que ser algo à parte do sistema que se pretende construir.

Criar condições de facilitação de acesso ao direito à portabilidade de dados, previsto inclusive pela LGPD, não deixa de ter importância. Todavia, o melhor caminho para tanto não parece ser o de criar facilidades e brechas para que dados sensíveis de cidadãos sejam explorados economicamente, em contradição àquilo que prevê a legislação. O direito à portabilidade de dados surge como possibilidade de retomada de controle do indivíduo sobre suas informações pessoais e como incentivo à concorrência entre empresas, e não como incentivo ao compartilhamento de informações sem necessidade ou finalidade que o justifique.

A Agência Nacional de Saúde Suplementar (ANS), em conjunto com a Autoridade Nacional de Proteção de Dados (ANPD), poderia exercer papel relevante nesse sentido, criando incentivos, estabelecendo normativas e auxiliando empresas prestadoras de serviços de saúde a melhorar as condições de acesso à portabilidade de dados. Poderia ser o caso, por exemplo, de se estabelecer padrões técnicos ou condições para que o compartilhamento de dados ocorra de maneira segura e facilitada para o consumidor.

3.2 O pilar assistencial: os dilemas de um banco integrado de dados de saúde

Se o pilar financeiro do Open Health esbarra em impossibilidades práticas e jurídicas, o pilar assistencial do sistema também mereceria reservas. A ideia de um amplo prontuário eletrônico integrado com informações de toda a população gera preocupações importantes relacionadas ao tratamento e armazenamento de informações dos indivíduos.

Hoje, no sistema de atenção básica à saúde pública, existe o Prontuário Eletrônico do Paciente (PEP). Criado em 2016 pela resolução n. 7 do Ministério da Saúde, o PEP funciona como registro de informações em relação aos atendimentos em Unidades Básicas de Saúde (UBS), armazenando informações clínicas e administrativas pertinentes ao paciente (Lima; Lima; Vale; Pisa, 2018). Esse, no entanto, é um sistema pertencente a um ramo específico da saúde pública, com regulamentação própria, de maneira a atender às necessidades da atenção básica à saúde.

No caso do Open Health, estaríamos falando de um sistema que agregaria informações pertinentes a todos os atendimentos médicos de um indivíduo, não apenas exclusivos à assistência básica de saúde. Busca-se, por meio do sistema, alcançar também atendimentos conduzidos por meio da saúde suplementar, dos hospitais e das redes privadas. A ideia por trás do sistema estaria em agregar, em um só lugar, diferentes bases de dados de prontuários eletrônicos e informações sobre o histórico médico de um indivíduo. Isso poderia envolver exames feitos, consultas marcadas, medicações tomadas, histórico de diagnósticos, entre outras possibilidades. Essas informações, por sua vez, poderiam ser compartilhadas por essas pessoas a diferentes instituições. A amplitude do sistema, portanto, seria muito maior que o PEP existente, hoje, no âmbito da saúde pública.

De acordo com Queiroga, a RNDS, instituída pela portaria n. 1.434/2020, serviria ao propósito de se tornar esse repositório. A RNDS foi criada com o objetivo de ser uma:

> [...] plataforma nacional voltada à integração e à interoperabilidade de informações em saúde entre estabelecimentos de saúde públicos e privados e órgãos de gestão em saúde dos entes federativos, para garantir o acesso à informação em saúde necessário à continuidade do cuidado do cidadão. (art. 254-A, Portaria n. 1.434/2020)

O programa foi criado como parte da Estratégia de Saúde Digital para o Brasil (2020-2028) (Ministério da Saúde, 2020), plano de ações relacionadas à inovação em saúde proposto pelo governo federal. Uma das prioridades no âmbito da Estratégia é a criação de um ambiente de interconectividade em saúde, que agregue: (i) serviços de telemedicina e telessaúde, públicos e privados, oferecidos via RNDS; (ii) serviços integrados de acompanhamento de pacientes crônicos; (iii) serviços para agendamento de consultas e exames; e (iv) serviços de extração de conhecimento para melhoria de diagnósticos, entre outras possibilidades

(Ministério da Saúde, 2020, p. 77). Esses pontos seriam alcançados por meio da promoção da interoperabilidade com a Atenção Primária à Saúde (APS), com laboratórios, com serviços de farmácia, com serviços de telessaúde e com serviços de regulação ambulatorial (Ministério da Saúde, 2020, p. 78-89). Em relação às farmácias, a Estratégia afirma que os benefícios podem alcançar "os meios de pagamento, a rastreabilidade dos medicamentos, o abuso de drogas e até mesmo, com o consentimento do paciente, o monitoramento da adesão ao tratamento" (Ministério da Saúde, 2020, p. 84).

A Estratégia também coloca como prioridade a criação de um ecossistema de inovação, por meio do desenvolvimento de iniciativas em Internet das Coisas (IoT), Big Data e uso secundário dos dados. Nesse sentido, afirma que "o futuro da saúde passa pela capacidade de armazenamento, processamento, organização, gestão e utilização desses conjuntos de dados oriundos das mais diversas fontes" e que o Ecossistema de Inovação seria um "catalisador de iniciativas inclusivas dos setores público e privado voltadas à utilização dos dados em saúde e de dispositivos inteligentes, que resultem no desenho e [na] utilização de soluções que apoiem profissionais e gestores de saúde" (Ministério da Saúde, 2020, p. 106). No âmbito do projeto, também estaria prevista a criação de um sistema chamado "Lago de Dados de Saúde", repositório de informações que permitiria que organizações acessassem informações advindas de fontes diversas – citam, como possibilidades: "sistemas públicos e privados de saúde, como registros eletrônicos de saúde, Prontuários Eletrônicos, registros de imunização, internações e altas hospitalares, assim como de sensores e aplicativos diversos" (Ministério da Saúde, 2020, p. 108).

Há, assim, já um embrião da ideia de Open Health em desenvolvimento no âmbito dos sistemas e das aplicações de saúde, considerando-se o incentivo previsto na Estratégia a sistemas de interoperabilidade entre saúde pública e privada e o investimento em práticas de análise integrada de dados.

Nessa esteira, cabe aqui um primeiro comentário a respeito da dificuldade de se colocar em prática sistemas como esse com atenção aos critérios de segurança da informação. A integração de tantos dados em um só local gera alarme em relação às possibilidades de acesso e segurança. Um sistema como esse seria fortemente visado por agentes maliciosos, já que conteria um agregado do histórico médico de todos os cidadãos brasileiros – algo cujo valor seria inestimável. Considerando-se que, hoje, já há casos relevantes de incidentes de segurança, envolvendo acesso

a dados armazenados pelo Ministério da Saúde[32], é necessário refletir sobre a possibilidade de sistemas como esse serem desenvolvidos sem riscos elevados.

Entender esses riscos, planejar e desenvolver ações possíveis para mitigá-los, seria medida prévia imprescindível anteriormente à implementação de um sistema como esse. Caberia, assim, ao Ministério da Saúde realizar estudo de análise de impacto à proteção de dados pessoais, para verificar se os eventuais benefícios da medida se justificariam em relação aos riscos que ela ofereceria para dados da população brasileira. Na Estratégia de Saúde Digital, há menção à necessidade de "estabelecer critérios legais e éticos para uso dos dados, respeitada a LGPD" (Ministério da Saúde, 2020, p. 108), bem como menção à necessidade de desenvolvimento de regulação aliada às regras e aos princípios previstos pela legislação (Ministério da Saúde, 2020, p. 34-35). Em nenhum ponto da estratégia, no entanto, há menção à elaboração de relatórios de impacto.

Em segundo lugar, aspectos relacionados à governança e ao controle do sistema também geram preocupação. Questões relacionadas ao Open Health não se encerram apenas em relação ao seu projeto e desenvolvimento, mas também à sua futura execução. Algumas perguntas se impõem diante dessa possibilidade: como ocorreria, a nível institucional, a possibilidade de integração entre diferentes bases de dados? Quais seriam as capacidades de controle e acesso às informações compartilhadas? Como ocorreria o fluxo de dados entre diferentes instituições? Que órgãos ficariam responsáveis pela governança, gestão e manutenção do sistema? Sendo um sistema que, a princípio, agregaria informações, no âmbito da saúde pública e privada, uma multiplicidade de atores deve estar envolvida e dialogando em consonância. Combinar interesses tão distintos no desenvolvimento de um único programa como esse seria um desafio por si só.

Dessa forma, a ideia de Open Health traz consigo inúmeros pontos nebulosos. No que tange à compatibilidade com a LGPD, há dissonâncias e desafios importantes colocados em ambas as vertentes do sistema que se pretende implementar. O projeto de um "cadastro positivo da saúde" não se sustenta do ponto de vista jurídico, uma vez que a LGPD vetou expressamente essa possibilidade. Ademais, um vasto prontuário eletrônico de cidadãos brasileiros que fosse aberto e compartilhável com empresas privadas esbarra em questões relevantes de segurança, governança e gestão do sistema. Sendo assim, os benefícios e mesmo o interesse público no desenvolvimento de um sistema como esse podem ser questionados à luz da legislação brasileira.

32 Em dezembro de 2020, dados de 243 milhões de brasileiros ficaram expostos após falha de segurança no âmbito de informações armazenadas pelo Conecte SUS, do Ministério da Saúde. Ainda em 2020, outro incidente de segurança expôs informações de 16 milhões de pessoas que tiveram covid-19. 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: 5 set. 2022.

Considerações finais

A ideia de Open Health é vislumbrada em um contexto crescente de inovações tecnológicas em saúde e finanças, criando uma esfera híbrida em que o compartilhamento de dados é o motor de geração de lucro de uma nova economia. Neste capítulo, buscou-se o contexto, as origens e as inspirações para um sistema como esse, de forma a entender quais seriam suas premissas e bases de implementação. Por fim, também foi analisada brevemente sua compatibilidade com a legislação brasileira sobre proteção de dados pessoais.

Há, pelo que foi levantado, duas principais inspirações para o Open Health: o sistema financeiro aberto (Open Banking), modelo de compartilhamento de dados aplicável ao setor financeiro, implementado no Brasil, a partir de 2020, e o modelo indiano da NDHM. Ambos evidenciam como a tarefa de se desenvolver um sistema como esse não é simples. O sistema financeiro aberto conta com robusta regulamentação, regras de estrutura regulatória e de governança. Para além dessa questão, o setor de saúde é bastante diverso do financeiro, contendo regras próprias tanto em relação à saúde pública como em relação à saúde suplementar, bem como múltiplas bases de dados dispersas. Integrar bases de dados, no âmbito da saúde, assim, seria tarefa diferente e possivelmente mais complexa que a de facilitar o compartilhamento de dados no âmbito do sistema financeiro. A iniciativa do governo indiano, por sua vez, tem sido criticada pelos seus impactos à privacidade de cidadãos e até mesmo pela possibilidade de exclusão de serviços de saúde daqueles sem o registro no banco de dados.

Ademais, quando se olha para a compatibilidade do sistema em relação à legislação brasileira sobre a proteção de dados, há dissonâncias relevantes. A ideia de um "cadastro positivo da saúde", vislumbrada para o sistema, não se sustenta juridicamente, uma vez que a prática de seleção de riscos a partir de informações de saúde é vedada pela legislação. Por outro lado, o plano de um repositório de dados de saúde de toda a população, que abarque também informações de atendimento na rede privada, traz consigo grandes preocupações relacionadas à ética no uso dos dados, à segurança da informação, à gestão e à governança do sistema. Qualquer iniciativa nesse sentido deveria ser precedida de análise de impacto à proteção de dados pessoais, de forma a avaliar a proporcionalidade entre riscos oferecidos pela aplicação e seus potenciais benefícios para cidadãos brasileiros.

Por fim, cabe dizer que facilitar o acesso à informação e o exercício do direito à portabilidade de dados no âmbito da saúde são objetivos importantes e

que devem ser incentivados. Todavia, o avanço em medidas de inovação em saúde deve ocorrer a partir de debates, cooperação institucional, avaliação de riscos e abertura à participação da sociedade civil. A tecnologia pode ser uma ferramenta útil e valiosa para melhoria na prestação de serviços e condições de atendimento à saúde da população brasileira, mas é necessário vê-la, também, com cautela, de forma a não entender determinadas soluções como milagrosas para problemas complexos. Por essas razões, diante de tantas questões prévias à sua implementação, a ideia de um sistema como o Open Health deveria ser vista com cautela.

Referências

ARAVINDAKSHAN**,** Sharngan. India's New National Digital Health Mission: A Trojan Horse for Privatization. **Center for Human Rights and Global Justice**. 14 dez. 2021. Disponível em: https://chrgj.org/2021/12/14/indias-new-national-digital-health-mission-a-trojan-horse-for-privatization/. Acesso em: 15 jun. 2023.

ATKINSON, Abbye. Rethinking Credit as Social Provision. **Stanford Law Review**, v. 71, p. 1093-1162, maio 2019. Disponível em: https://review.law.stanford.edu/wp-content/uploads/sites/3/2019/05/Atkinson-71-Stan.-L.-Rev.-1093-2019.pdf. Acesso em: 15 jun. 2023.

BANCO CENTRAL DO BRASIL. BCB. BC põe em consulta pública regras para funcionamento do Open Banking. 10 dez. 2019. Disponível em: https://www.bcb.gov.br/detalhenoticia/392/noticia. Acesso em: 5 set. 2022.

BANCO CENTRAL DO BRASIL. BCB. Circular nº 4.032, de 23 de junho de 2020. Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/51077/Circ_4032_v3_P.pdf. Acesso em: 5 set. 2022.

BRASIL. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 15 jun. 2023.

BRASIL. Ministério da Saúde. Gabinete do Ministro. Portaria n. 1.434/2020, 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. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-1.434-de-28-de-maio-de-2020-259143327. Acesso em: 15 jun. 2023.

CARMEN, Gabriela Del. 15 healthtechs que estão revolucionando a saúde para ficar de olho em 2021. **Forbes**, 30 jul. 2021. Disponível em: https://forbes.com.br/forbes-tech/2021/07/16-healthtechs-que-estao-revolucionando-a-saude-para-ficar-de-olho-em-2021/#foto6. Acesso em: 5 set. 2022.

CARRUTHERS, Bruce G. Financialization and the institutional foundations of the new capitalism. **Socio-Economic Review**, v. 13, n. 2, p. 379-398, 2015. DOI: 10.1093/ser/mwv008. Acesso em: 15 jun. 2023.

CHAKRABORTY, Imon; ILAVARASAN, Vigneswara P.; EDIRIPPULIGE, Sisira. Health-tech startups in healthcare service delivery: A scoping review. **Social Science & Medicine**, [s.l.] 2021. DOI: 10.1016/j.socscimed.2021.113949. Acesso em: 15 jun. 2023.

CHARRON-CHÉNIER, Raphaël; SEAMSTER, Louise. Racialized Debts: Racial Exclusion From Credit Tools and Information Networks. **Critical Sociology**, v. 47, n. 6, p. 977-992, 2021. DOI: https://doi.org/10.1177/0896920519894635. Acesso em: 15 jun. 2023.

CHRISTOPHERS, Brett. The limits to financialization. **Dialogues in Human Geography**, v. 5, n. 2, p. 183-200, 2015. DOI: https://doi.org/10.1177/2043820615588153. Acesso em: 15 jun. 2023.

CROUCH, Colin. Privatised Keynesianism: An Unacknowledged Policy Regime. **The British Journal of Politics and International Relations**, v. 11, n. 3, p. 382-399, 2009. Disponível em: https://pure.mpg.de/rest/items/item_1232424/component/file_2030504/content. Acesso em: 15 jun. 2023.

EPSTEIN, Gerald A. (Ed.). Introduction: Financialization and the World Economy. *In*: EPSTEIN, Gerald A. (Ed.) **Financialization and the World Economy**. Cheltenham; Northampton: Edward Elgar Publishing, 2005.

EUBANKS, Virginia. **Automating inequality**: how high-tech tools profile, police, and punish the poor. 1. ed. Nova Iorque: St. Martin's Press, 2017.

FELIX, Paula. CFM regulamenta telemedicina; veja novas regras. **Veja**, 13 jul. 2022. Disponível em: https://veja.abril.com.br/saude/cfm-regulamenta-telemedicina-veja-novas-regras/. Acesso em: 5 set. 2022.

G1. Open Banking agora será Open Finance, diz Banco Central. 24 mar. 2022. Disponível em: https://g1.globo.com/economia/open-banking/noticia/2022/03/24/open-banking-agora-sera-open-finance-diz-banco-central.ghtml. Acesso em: 5 set. 2022.

HEIJLEN, Roel; CROMPVOETS, Joep. Open Health Data: mapping the ecosystem. **Digital Health**, jan. 2021. DOI: 10.1177/20552076211050167. Disponível em: https://pubmed.ncbi.nlm.nih.gov/34777853/. Acesso em: 5 set. 2022.

JAIN, Sudeep; GABOR, Daniela, The Rise of Digital Financialisation: The Case of India. **New Political Economy**, v. 25, n. 5, p. 813-828, jul. 2020. DOI: https://doi.org/10.1080/13563467.2019.1708879. Disponível em: https://www.tandfonline.com/doi/full/10.1080/13563467.2019.1708879. Acesso em: 5 set. 2022.

KRIPPNER, Greta R. Democracy of Credit: Ownership and the Politics of Credit Access in Late Twentieth-Century America. **American Journal of Sociology**, v. 123, n. 1, p. 1-47, jul. 2017. DOI: https://doi.org/10.1086/692274. Disponível em: https://www.journals.uchicago.edu/doi/full/10.1086/692274. Acesso em: 5 set. 2022.

LAVINAS, Lena. The Takeover of Social Policy by Financialization: The Brazilian Paradox. Nova York: Palgrave Macmillan, 2017.

LAVINAS, Lena; ARAÚJO, Eliane; BRUNO, Miguel. "Brasil: vanguarda da financeirização entre os emergentes? Uma análise exploratória". Texto para Discussão, n. 32, 2017. Instituto de Economia da Universidade Federal do Rio de Janeiro. Disponível em: Disponível em: http://www.ie.ufrj.br/images/pesquisa/publicacoes/discussao/2017/tdie0322017lavinasaraujobruno.pdf. Acesso em: 5 set. 2022.

LIMA, V. S.; LIMA, V. S.; VALE, T. M. do; PISA, I. T. Prontuário eletrônico do cidadão: desafios e superações no processo de informatização. **Revista de Saúde Digital e Tecnologias Educacionais**, Fortaleza, v. 3, número especial, p. 100-113, 2018. Disponível em: http://periodicos.ufc.br/resdite/article/view/39756/95752. Acesso em: 5 set. 2022.

MATHESON, John H. The Equal Credit Opportunity Act: A Functional Failure. **Harvard Journal on Legislation**, v. 21, p. 371, 1984. Disponível em: https://scholarship.law.umn.edu/faculty_articles/132/. Acesso em: 5 set. 2022.

MINISTÉRIO DA SAÚDE. **Estratégia de Saúde Digital para o Brasil 2020-2028**. Ministério da Saúde: Brasília, 2020. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf. Acesso em: 4 jul. 2022.

NOBLE, Safiya Umoja. **Algorithms of oppression**: how search engines reinforce racism. Nova Iorque: New York University Press, 2018.

PASQUALE, Frank. **The black box society**: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

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

SAWYER, Malcolm. What is Financialization? **International Journal of Political Economy**, v. 42, n. 4, p. 5-18, 2013. Disponível em: https://www.jstor.org/stable/24696306. Acesso em: 5 set. 2022.

SHRIVASTAVA, Rishabh. Why you may be having a national digital health ID without even asking for it. **Citizen Matters**. 18 out. 2021. Disponível em: https://citizenmatters.in/explainer-national-digital-health-id-privacy-concerns-27828. Acesso em: 5 set. 2022.

STIGLITZ, Joseph E.; WEISS, Andrew. Credit Rationing in Markets with Imperfect Information. **The American Economic Review**, v. 71, n. 3, p. 393-410, jun. 1981. Disponível em: https://www.jstor.org/stable/1802787. Acesso em: 5 set. 2022.

ZACHARIADIS, Markos; OZCAN, Pinar. The API Economy and Digital Transformation in Financial Services: The Case of Open Banking. **SWIFT – Institute Working Paper**, n. 2016-001, jul. 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199. Acesso em: 5 set. 2022.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. Londres: Profile Books, 2019.

https://doi.org/10.29397/EdicoesLivres/20250108

“CPF pra desconto?”: uma perspectiva dos direitos à saúde, à defesa do consumidor e à proteção de dados em farmácias

Matheus Zuliane Falcão
Marina Fernandes
Camila Leite
Rodrigo Murtinho

O presente artigo busca analisar criticamente a prática comercial difundida e conhecida do varejo farmacêutico brasileiro de coletar dados pessoais para finalidades adversas ao cumprimento de obrigações legais ou regulatórias, especialmente o Cadastro de Pessoas Físicas (CPF). Na primeira seção, apresenta-se uma breve revisão sobre como os dados de saúde podem ser usados no contexto da economia digital, inclusive de forma contrária aos interesses de seus titulares, com foco especial no varejo farmacêutico. Na segunda parte, apresenta-se uma leitura da saúde digital baseada em direitos, indicado que o direito à saúde, o direito à proteção de dados pessoais e a defesa do consumidor já constituem sistemas jurídicos com desdobramentos nítidos para o uso de dados em saúde, particularmente no caso concreto do varejo farmacêutico. Na terceira parte, apresenta-se uma descrição histórica, feita com revisão documental e de notícias, sobre os passos dados até o momento para proteção jurídica de usuários contra o uso indevido de dados no varejo. Finalmente, a última parte é dedicada a uma análise crítica sobre tal percurso institucional, com base nos elementos descritos nas duas primeiras seções.

1. Função econômica: economia política de dados e saúde

A transformação digital da saúde está substancialmente associada a inovações tecnológicas que possibilitam coleta massiva de dados, armazenamento em grandes bases e transformação automatizada em informação, por meio de Inteligência Artificial (IA), principalmente aprendizagem de máquina (Fornazin, Marcelo *et al.*, 2021). Transformar essas informações em ações de saúde, tanto a nível populacional

quanto na prática clínica, traz grande potencial para os sistemas de saúde, bem como riscos para usuários, a depender do uso (Panch, Trishan *et al.*, 2019).

A transformação de elementos da realidade em dados processáveis em computador está associada tanto à capacidade de coletar esses dados, por meio de sensores ou de sistemas de informação, quanto ao aumento da capacidade de computadores de armazená-los e processá-los. No caso da saúde, esses sensores podem estar em telefones portáteis (aplicativos de saúde e bem-estar, geolocalização etc.) ou em dispositivos médicos conectados (glicosímetros e bombas de insulina), por exemplo. Já os Sistemas de Informação em Saúde (SIS) incluem prontuários eletrônicos digitais e outros dados coletados em serviços de saúde, por exemplo, farmácias.

A economia política de dados e saúde envolve a análise dos agentes econômicos e interesses envolvidos na dinâmica que inclui o tratamento desses dados. Há grande interesse econômico nessa área, por diferentes razões, convém conhecê-las e considerá-las em análises setoriais.

1.1 Dados de saúde para perfilização do setor de seguros de saúde

Uma das principais discussões em torno do uso de dados de saúde no setor de seguros é estabelecer o quanto cada pessoa representa em termos de risco financeiro com base em suas características genéticas, seus hábitos e outros fatores que influenciam em sua saúde. Isso é feito especialmente por via de ferramentas de IA que são capazes de predizer o risco que um usuário representa, a partir de seus dados clínicos e comportamentais (Bates, David W. *et al*., 2014).

A recusa de incluir uma pessoa no seguro com base em seu risco ou mesmo o arbitramento de preços diferenciados a partir desse critério é o que se chama de seleção de risco (Hsiao, William C., 2003). Em outros setores de seguro, como o automotivo, a prática é comum, uma vez que permite precificar o seguro de acordo com o perfil do consumidor. No mercado de saúde, no entanto, a prática apresenta graves problemas éticos e viola direitos, sendo vedada no Brasil.[33]

Os problemas associados à seleção de risco no mercado de saúde são a quebra do caráter de mutualismo no contrato de saúde, particularmente importante nesse

33 A seleção de risco é expressamente proibida pela Lei Geral de Proteção de Dados Pessoais (LGPD), em seu artigo 11, §5º. Antes da aprovação da LGPD, desde 2017, a Agência Nacional de Saúde Suplementar (ANS) já tinha uma súmula interpretativa que igualmente proibia a seleção de risco. Inclusive, a vedação à seleção de risco pode ser considerada como um princípio norteador da atividade econômica do país. Ao considerar a assimetria informacional (art. 51, §1º, CDC) e a vulnerabilidade do consumidor (art. 4º, inciso I, CDC), a precificação com base no risco se constitui como uma vantagem manifestadamente excessiva (art. 29, inciso V, CDC). Também deve-se considerar o direito básico de igualdade na contratação (art. 6º, inciso II, CDC) que não admite a precificação discriminatória.

setor, pois as pessoas não têm condições de prever ou mesmo de saber suas necessidades em saúde, isto é, exatamente de qual tratamento precisam. Então, a existência do seguro está fundamentada na ideia de diluição do risco, isto é, agrupar pessoas com contribuições financeiras periódicas para evitar grande dispêndio em momentos de necessidade de saúde.

Além disso, essas necessidades são moldadas largamente pelo ambiente em que as pessoas se encontram, conforme preceituado pela ideia de determinação social de saúde, que muito dialoga com o campo da saúde coletiva (Fleury-Teixeira, Paulo, 2009), ou mesmo pela ideia de determinante social de saúde adotada pela Organização Mundial de Saúde (OMS) (WHO, 2009). Trata-se aqui da proposição de que a condição de saúde é determinada socialmente, e não individualmente, isso faz com que as pessoas sejam responsabilizadas por sua condição de saúde, o que significa ampliar vulnerabilidades já existentes.

1.2 Dados de saúde para inovação tecnológica no setor farmacêutico: evidência de mundo real e testes clínicos

Dados de saúde são o principal combustível para o funcionamento da inovação em saúde digital, especialmente a partir dos avanços no campo da IA. Tais ferramentas permitem a análise de grandes bases de dados para inferir conclusões importantes. Assim, mesmo bancos de dados de grandes dimensões, que ainda demandam várias etapas de pré-tratamento de dados, podem conter grande utilidade em termos de informações sob a gestão de uma empresa ou entidade com capacidade computacional e força de trabalho para tratá-los (WHO, 2024).

Um caso particularmente interessante está no setor farmacêutico, em que muitos recursos são despendidos anualmente em inovação. A descoberta de medicamentos e vacinas geralmente envolve uma etapa pré-clínica, em que se busca encontrar um novo composto químico para realização de testes *in vitro*, e uma etapa clínica, posterior e mais avançada, em que o novo produto é testado em seres humanos para aferir sua segurança, sua qualidade e sua eficácia. Uma vez aprovado para comercialização, por via do registro farmacêutico, as empresas seguem monitorando seu uso, especialmente para encontrar efeitos adversos, na etapa de pós-mercado.

Dados de saúde contêm elevado potencial em tal processo, tanto para se encontrar potenciais participantes de pesquisa para testes clínicos quanto para se descobrir novas informações, a partir de dados sobre uso em tempo real. Encontrar esses participantes é uma tarefa custosa, especialmente dentro da tendência de mercado atual de enfoque em doenças raras que geram mais retornos financeiros para as

empresas. Frequentemente, buscam-se perfis muitos específicos de pessoas, por exemplo, idosos com uma condição específica e utilizando um medicamento em particular. Assim, grandes bases de dados podem ser de interesse do setor.

Além disso, a consolidação de grandes bancos de dados sobre a realidade de serviços clínicos, incluindo farmácias, permite gerar evidências sobre o que está acontecendo nesses espaços. São as chamadas evidências de mundo real e servem tanto para comprovar segurança e eficácia de medicamentos quanto para se encontrar novas indicações terapêuticas, além de apresentarem grande potencial para a inovação farmacêutica, incluindo dados sobre consumo de fármacos (Dagenais, Simon *et al.*, 2022).

1.3 Dados de saúde para inovação tecnológica em IA: treino de algoritmos

Para além do uso de dados no processo de inovação farmacêutica, a aplicação de IA à saúde aumenta cada vez o valor de grandes bancos de dados de saúde para outro processo: treinamento de algoritmos. O desenvolvimento de ferramentas dessa natureza envolve validação e repetição com dados da realidade e quanto mais variada for a base de dados, maior é sua precisão e acurácia.

Assim, grandes bancos de dados de saúde fornecem potencial econômico para desenvolvimento de algoritmos com potencial aplicação em diferentes áreas. Por exemplo, comercial (um aplicativo para identificar padrões de consumo), clínica (um aplicativo capaz de propor tratamentos mais eficazes com base em desfechos clínicos) ou populacionais (a relação entre um fator ambiental e o consumo de um determinado medicamento).

1.4 Dados de saúde para *marketing* personalizado

Uma das principais atividades econômicas com dados pessoais é o *marketing* personalizado, isto é, a oferta de anúncios publicitários com base em padrões de comportamento. Essa é, inclusive, a fonte principal do faturamento de grandes empresas de tecnologia.

Dados de saúde dizem muito sobre o perfil de consumo que uma pessoa pode apresentar, por exemplo, uma pessoa que consome medicamentos para diabetes, frequentemente estará interessada em um glicosímetro. A compra de um teste de gravidez pode indicar a necessidade de outros produtos para o período pré-natal. Assim, há grande potencial para publicidade direcionada.

No caso do setor farmacêutico, o uso de dados contém uma componente adicional, que é a publicidade farmacêutica direcionada não a consumidores,

mas a prescritores de medicamentos. Grande parte dos recursos publicitários da indústria são dedicados a essa atividade, considerando a relevância da indicação profissional na escolha do usuário.

1.5 Dados de saúde para organização logística

Finalmente, dados de saúde podem ter uma função econômica útil para os setores público e privado na organização das cadeias de suprimento de produtos de saúde, por exemplo, medicamentos. As empresas podem se beneficiar de dados de consumo para organizar melhor a cadeia produtiva, otimizando seus gastos logísticos, de acordo, por exemplo, com a quantidade esperada de consumo de um determinado produto em uma região específica.

2. Uma abordagem a partir dos direitos

Para que o potencial da transformação digital seja completamente executado é fundamental construir um meio legal e regulatório que mitigue os riscos, por exemplo, vieses algorítmicos e incidentes de segurança, e assegure proteção contra usos indevidos, como discriminação baseada em condições de saúde, exploração econômica sem consentimento ou transparência.

Assume-se aqui uma perspectiva dos direitos não como um sistema estático, do qual se retiram regras e princípios, mas, sim, como um sistema contínuo que reflete as lutas sociais e as disputas em torno de sua afirmação retratadas na incidência da sociedade, nas decisões estatais e nas afirmações da democracia e da cidadania (Stevanim, Luiz Felipe; Murtinho, Rodrigo, 2021). Essa ideia tem lastro em Coutinho que afirma que:

> [...] o direito é, de certo modo, algo que antecede – e é mais amplo – do que o direito positivo, ou seja, do que o direito estatuído nas Constituições, nos códigos etc. Os direitos têm sempre sua primeira expressão na forma de expectativa de direito, ou seja, de demandas que são formuladas, em dado momento histórico determinado, por classes ou grupos sociais. (Coutinho, 2008, p. 54)

2.1 O direito à saúde

O direito à saúde, fruto da Reforma Sanitária (Cohn, Amélia, 1989), está cristalizado na Constituição Federal e contém os princípios da universalidade, da integralidade

e da participação comunitária. A equidade e a descentralização também são comumente incluídas nesse conjunto. Ainda de acordo com a Constituição, sua realização se dá por meio do Sistema Único de Saúde (SUS), que compõe as diversas ações e serviços de saúde executadas pelo Estado brasileiro, a nível federal, municipal e estadual.

O uso de dados no SUS pode se dar de diferentes maneiras. Para os fins deste capítulo, no entanto, vale explorarmos os elementos mais conceituais do direito à saúde que resvalam, inclusive, nas relações privadas, particularmente em dois de seus elementos: a não discriminação e a redução do risco.

A não discriminação é parte central do direito à saúde dentro da teoria dos direitos humanos e está inscrita em documentos internacionais (CESCR, 2000). Além disso, pode-se estabelecer uma relação entre não discriminação e a ideia de equidade e de universalidade.

No contexto do uso de dados pessoais, esse princípio está especialmente associado ao mal uso de dados pessoais, que podem impactar negativamente as pessoas, por exemplo, por via de perfilização de risco, fazendo quem está mais vulnerável à doença a pagar mais por seguro de saúde.

Outra questão associada à não discriminação é o risco emergente de vieses associados ao uso de IA em saúde, uma vez que essas ferramentas geralmente aprendem com dados que refletem práticas humanas que contêm vieses por si só, como o racismo (Silva, Tarcízio, 2022; Baptista, Daiane, 2023). Além disso, a própria indisponibilidade de dados sobre populações específicas pode levar a vieses, aprofundando ainda mais iniquidades já existentes.

Uma das formas que o direito tem de lidar com essas questões é a regulação sanitária, que no Brasil também está sob a guarida do direito à saúde e do SUS, por exemplo, por via do Sistema Nacional de Vigilância Sanitária (SNVS), que tem a Agência Nacional de Vigilância Sanitária (Anvisa) como seu vértice.

As ações regulatórias estão inscritas na ideia de redução do risco, presente também na Constituição. O SNVS atua para reduzir o risco associado a produtos e a serviços de saúde. Com o uso crescente de dados pessoais em produtos de saúde, por exemplo, *softwares* como dispositivos médicos (SaMD[34]), a regulação passa a incluir, dentro do paradigma da segurança e da eficácia desses produtos, questões associadas à saúde digital, intercalando-se inclusive com um novo direito emergente que é o direito à proteção de dados pessoais.

34 Resolução 751, de 2023, da Anvisa.

2.2 O direito à proteção de dados pessoais

Ainda que a Constituição já trouxesse o direito à privacidade e o Código de Defesa do Consumidor trouxesse disposições sobre banco de informações, essas disposições se viam limitadas aos desafios da transformação digital. A necessidade da regularização dos fluxos de dados, aliada à necessária proteção de titulares de dados, gerou a demanda da criação de um panorama regulatório para a proteção de dados. Com isso, surgiu a Lei Geral de Proteção de Dados Pessoais (LGPD – lei n. 13.709/2018), cuja vigência foi iniciada em 2020 e cuja aplicação é realizada essencialmente pela Autoridade Nacional de Proteção de Dados (ANPD), que a regulamenta.

A ideia de proteção de dados pessoais é baseada em autonomia, transparência e não discriminação. Concretamente, possui disposições relevantes sobre saúde, como a definição de dados de saúde como sensíveis, as possibilidades de tratamento de dados de saúde sem consentimento e a vedação à seleção de risco em planos de saúde. Entretanto, essas disposições ainda carecem de regulamentação.

Ademais, a proteção de dados foi considerada relevante a ponto de ser incluída no rol de direitos fundamentais do art. 5º, inciso LXXIX, após a aprovação da emenda constitucional n. 115/2022.

3. Mapeamento do mercado

O mercado da saúde digital, no qual circulam os dados de saúde, é amplo e deve ser compreendido de acordo com a sua complexidade. É difícil precisar a função econômica de cada agente, considerando as novas dinâmicas da economia da informação, conforme explicado por Sergio Amadeu Silveira *et al*., 2016. Com a entrada de empresas do setor de tecnologias digitais no setor da saúde, o retrato fica ainda mais complexo. Convém, no entanto, identificar ao menos alguns atores-chave do setor.

O CPF, ainda que não seja um dado pessoal sensível, quando observado de forma individualizada, representa o tratamento de dados de saúde nesse ecossistema, especialmente quando cruzado com outros dados como quais medicamentos uma pessoa adquire ou qual é a unidade de saúde na qual ela recebeu a receita. É através do CPF, e em torno dele, que são agregados dados diversos de cada cidadão.

O varejo farmacêutico, formado pelas farmácias e drogarias privadas, forma a primeira camada desse mercado, responsável especialmente pela coleta de dados

pessoais no momento da compra. Os interesses comerciais, no entanto, vão para muito além do varejo por si só. Uma empresa desse setor pode estar associada (por meio de parcerias e programas comuns) ou mesmo pertencer ao mesmo grupo econômico de outros varejistas, por exemplo, o setor de supermercados.

Além disso, uma empresa de varejo farmacêutico pode exercer as funções de distribuição de medicamentos e, em alguns casos, mesmo de fabricação, compondo também a indústria farmacêutica. Tais casos são exceções, mas há empresas existentes no país que preenchem essas três funções e que têm grande relevância econômica, por exemplo, o Grupo Dimed (Panvel, Dimed e Laboratórios Lifar) e o Grupo RD.

Ainda que não seja a mesma empresa ou o mesmo grupo econômico, farmácias privadas podem atuar de maneira colaborativa com outras empresas do setor, por exemplo, realizando cadastros para a indústria farmacêutica, o que acontece especialmente para medicamentos de uso contínuo, por exemplo, liraglutida e semaglutida (nome de referência: Ozempic), usadas no contexto do tratamento do diabetes e para obesidade.

Há que se falar ainda de uma distinção relevante entre as empresas que compõem a indústria farmacêutica, os laboratórios produtores de genéricos e os laboratórios produtores de medicamentos inovadores. O faturamento da indústria nacional vem majoritariamente da venda de genéricos e similares, enquanto grandes transnacionais farmacêuticas exploram o mercado de medicamentos protegidos por patentes, que geralmente também são os medicamentos de referência (Paranhos, Julia; Mercadante, Eduardo; Hasenclever, Lia, 2020). Essa realidade, no entanto, vem sendo alterada, nos últimos anos, com maior participação do capital privado nacional em atividades de pesquisa e desenvolvimento.

No setor de serviços de saúde, há operadoras de planos de saúde e administradoras de benefícios. Enquanto as primeiras são responsáveis por planos privados de assistências podendo ou não ter uma rede própria, as administradoras funcionam como intermediárias entre pessoas jurídicas que contratam planos de saúde e operadoras, exercendo funções como administração de carteiras, corretagem, negociação de reajustes etc.

De forma similar, há também no varejo de medicamentos, em particular, empresas que fazem a gestão de benefícios, administrando contratos e programas de desconto. Em outros países, como nos Estados Unidos da América, essas empresas têm uma função ainda mais relevante – atuam como intermediárias entre seguradoras de saúde ou grandes hospitais e a própria indústria farmacêutica.

Finalmente, dentro do contexto da transformação digital, novas empresas adquirem relevância, aquelas que administram serviços de suporte digital a serviços de saúde, por exemplo, plataformas para exercício da telessaúde, para receituário digital ou para gestão de prontuários eletrônicos.

A heterogeneidade dos agentes econômicos que atuam direta ou indiretamente no varejo farmacêutico é um dos fatores que dificulta a compreensão do fluxo de dados no setor. A atuação verticalizada desses agentes, os diversos interesses econômicos envolvidos e a falta de transparência e enforcement dos direitos à proteção de dados e defesa do consumidor aprofundam as assimetrias informacionais, potencializam os riscos de uso discriminatório de dados pessoais e dificultam o acesso à saúde.

4. Histórico de ações concretas em torno da coleta de dados pessoais no varejo farmacêutico

O avanço do tema da proteção de dados na saúde, entretanto, se dá não somente pelos direitos já consolidados. Mas por demandas sociais construídas pela sociedade civil e pelo Ministério Público Federal (MPF), no seu papel de defesa de direitos coletivos e difusos.

Uma das primeiras movimentações públicas em torno da coleta de dados pelo setor farmacêutico ocorreu em janeiro de 2018. Na ocasião, o Ministério Público do Distrito Federal e Territórios (MPDFT) iniciou um inquérito civil público para investigar uma possível venda de dados pessoais coletados por farmácias para empresas de plano de saúde e de análise de crédito (Luiz, Gabriel, 2018).[35] Situada na Comissão de Dados Pessoais do MPDFT, o objetivo da investigação era compreender o fluxo de dados para descobrir o que as farmácias fazem com os dados sensíveis dos consumidores. O estudo realizado no Inquérito, sugerindo aparente falta de adequação e de atualização dos grupos farmacêuticos em relação à LGPD e a regimes de adequação corporativa, foi utilizado pela ANPD na realização de sua própria investigação sobre o assunto.

Já em agosto de 2018, após representação do Instituto de Referência em Internet e Sociedade (Iris, 15 ago. 2018), o Ministério Público de Minas Gerais (MPMG) iniciou uma investigação preliminar para avaliar possíveis violações na coleta e no tratamento de dados nas drogarias Raia, Pague Menos, Pacheco e Onofre.[36] Já no âmbito de um processo administrativo, em setembro de 2018, o MPMG celebrou

35 Inquérito civil público n. 08190.030923/19-55, do Ministério Público do Distrito Federal e Territórios.

36 Investigação preliminar n. 0024.18.010995-1, do Ministério Público do Estado de Minas Gerais.

um Termo de Ajustamento de Conduta (TAC) com a Drogaria Araujo.[37] Na ocasião, o MPMG considerou que a falta de informação e de transparência aos consumidores na coleta de seus dados pessoais, especialmente quanto à finalidade da coleta, caracterizavam conduta abusiva (Iris, 3 dez. 2018).

O TAC exigia que a rede farmacêutica adequasse seu programa de fidelidade para o cadastro ocorrer apenas pela via virtual, de forma que no balcão os vendedores deveriam se limitar a perguntar se o consumidor era ou não cadastrado no programa de fidelidade. Com isso, a coleta de dados deveria ser restrita à "identificação dos consumidores aderentes ao programa no momento do cadastro e quando da sua ativação para fins de percepção do desconto/promoção" (Ministério Público de Minas Gerais, 2018),[38] de forma a ser necessário o consentimento específico para eventual compartilhamento de dados com outras empresas (Minas Gerais, 2018).[39] Além disso, o termo também impunha critérios de transparência e informação aos usuários.

Já em julho de 2021, o Instituto Brasileiro de Defesa do Consumidor (Idec) e o Procon de São Paulo notificaram a Droga Raia e a Drogasil, integrantes do grupo econômico RD, questionando a coleta de biometria para concessão de descontos, a licitude do consentimento e a falta de transparência e informações claras e adequadas (Idec, 2021). Após os questionamentos, o grupo RD desistiu de coletar dados biométricos, mas não explicou a necessidade específica de coleta da biometria e do CPF e a finalidade do tratamento de dados (Knoth, Pedro, 2021). Na ocasião, o Idec também enviou uma carta à Associação Brasileira de Farmácias e Drogarias (Abrafarma) para saber se outras empresas também estavam coletando dados biométricos dos consumidores.

Na mesma época e com a LGPD já em vigência, o Procon do Mato Grosso multou a Rede de Farmácias Raia/Drogasil pela coleta irregular de dados pessoais (Governo de Mato Grosso, 2021). O Procon compreendeu que o consentimento dos titulares-consumidores para o tratamento de seus dados pessoais era irregular, pois, diante da falta de informações claras e adequadas, eles não tinham ciência sobre a finalidade do tratamento.

Em novembro de 2021 a discussão passou a ter âmbito nacional, quando a Secretaria Nacional do Consumidor (Senacon/MJ) deu início a uma Averiguação Preliminar de Irregularidade para investigar a solicitação do CPF para concessão de descontos. Com o objetivo de apurar se as farmácias violaram a LGPD, a Secretaria enviou

37 Processo administrativo n. 0024.18.002027-3, do Ministério Público do Estado de Minas Gerais.

38 Cláusula Terceira do TAC firmado entre o MPMG, por meio do Programa PROCON-MG, e a Drogaria Araújo.

39 Minas Gerais. Ministério Público do Estado de Minas Gerais. Investigação preliminar n. 0024.18.002027-3. Belo Horizonte, 18 set. 2018.

questionamento às cinco principais redes de drogarias do país: Raia/Drogasil, Pacheco, São Paulo, Pague Menos e Panvel (Longuinho, Daniella, 2021).[40]

Com exceção da atuação do MPDFT, todas as movimentações citadas estão principalmente relacionadas à defesa de consumidores. O que é possível de ser observado tanto pelo escopo de atuação dos órgãos responsáveis pela condução das investigações[41] quanto pelo objeto investigado – em geral, os focos da investigação são a transparência, a informação e o consentimento. Em razão da necessidade de discutir aspectos relacionados à proteção de dados com mais profundidade, durante uma audiência pública na Comissão de Defesa do Consumidor (CDC) da Câmara dos Deputados em 26 de abril de 2023,[42] a ANPD foi instada pelo Idec e por deputados federais a publicar os resultados de sua pesquisa sobre a coleta de dados em farmácias.

Então, em maio de 2023, a ANPD tornou público um estudo exploratório sobre o tratamento de dados pessoais pelo varejo farmacêutico. A relevância do estudo foi justificada pela denúncia do MPDFT, pela notificação do Idec ao grupo RD e pela investigação e pelo TAC do MPMG. Na nota técnica n. 4/2023, a autoridade demonstrou, a partir de seu estudo, que os dados são tratados para finalidades diferentes daquelas informadas aos titulares (participação em programas de fidelização) e que há compartilhamento de dados com prestadoras de serviço para fins de perfilização (ANPD, 2023). Na ocasião, a autoridade também instaurou procedimento fiscalizatório através da Coordenação-Geral de Fiscalização em face da Raia/Drogasil, do programa Stix Fidelidade e Inteligência e da Federação Brasileira das Redes Associativistas e Independentes de Farmácias (Febrafar).[43] O procedimento tem o propósito de garantir que essas empresas estejam em conformidade com as regulamentações de proteção de dados, como a LGPD, visando proteger a privacidade e os direitos dos cidadãos.

O Idec enviou ofícios a Senacon e a ANPD com contribuições sobre o uso do CPF no varejo farmacêutico e solicitou sua habilitação como interessado e a elaboração de um plano de atuação conjunta entre as autoridades, em vista do trâmite de processos administrativos de mesmo objeto em ambas autoridades.

Para além dos problemas tradicionalmente relacionados à defesa de consumidores e à proteção de dados, a coleta de dados no setor farmacêutico também levanta preocupações quanto ao acesso aos medicamentos. Na audiência pública sobre

40 Averiguação preliminar de irregularidade n. 08012.003147/2021-67, da Secretaria Nacional do Consumidor.

41 Nas situações em que os consumidores também sejam titulares de dados, a Senacon e os Procons também terão competência para aplicar as normas previstas na LGPD (Cf.: Mendes, Laura Schertel; Doneda, Danilo, 2018).

42 Disponível em: https://www.youtube.com/watch?v=ZYJg-AT1kmU. Acesso em: 14 fev. 2024.

43 Processo de fiscalização n. 00261.001371/2023-32, da Autoridade Nacional de Proteção de Dados.

a regulação do preço de remédios no Brasil, que ocorreu na CDC em 13 de dezembro de 2023, o Idec demonstrou como a concessão de descontos, mediante o fornecimento do dado pessoal, reflete uma falha de mercado na precificação dos medicamentos.[44]

Como ocorre em muitos países, o preço de medicamentos no Brasil é regulado. Tal regulação, com fundamento na lei n. 10.742, de 2003, se dá pela definição de preços máximos autorizados para cada medicamento, também chamados de preços teto. A regulação e a fiscalização são feitas pela Câmara de Regulação do Mercado de Medicamentos (Cmed), autoridade sob jurisdição dos ministérios da Fazenda, da Saúde e da Justiça e com secretária executiva na Anvisa. A regulação é frequentemente criticada por estabelecer tetos muito elevados, que não correspondem à realidade do mercado, levantando inclusive a hipótese de que os descontos fornecidos no ato de compra são artificiais, uma vez que são dados sobre esse preço regulado e não sobre o preço de mercado (Souza, Caroline Miranda Alves de; Paranhos, Julia; Hasenclever, Lia, 2021; Miziara, Nathália Molleis, 2013).

Na ocasião da audiência pública foi apresentada a pesquisa "Remédio a preço justo", publicada em março de 2023, que demonstrou que, em média, o compartilhamento do CPF rendeu um desconto de 25% para os medicamentos de marca, correspondendo a R$82,91 em valores reais (Idec, 2023). Sendo que a diferença entre o preço teto para um dos medicamentos pesquisados e o desconto efetivamente praticado chegou a 223,89%.

Uma série de matérias publicadas pelo portal Uol, em setembro de 2023, sob assinatura da jornalista Amanda Rossi, apresentam conclusões similares como: (i) a suposta concessão de descontos está intimamente atrelada ao fornecimento de um dado pessoal, o CPF do consumidor; e (ii) o suposto desconto, na realidade, é um reflexo distorcido do preço estipulado pelas próprias farmácias, observado o teto da Cmed (Rossi, Amanda, 1 set. 2023a, 2023b, 2023c, 2023d). Além disso, a jornalista também traz informações relevantes sobre o fluxo de dados no varejo farmacêutico, como a utilização dos dados para perfilização e para *marketing* personalizados.

Tais reportagens chamaram novamente a atenção do Ministério da Justiça que notificou, em outubro de 2023, a Raia/Drogasil, por meio da Senacon/MJ, a apresentar esclarecimentos sobre o uso de dados pessoais de seus clientes. Segundo Amanda Rossi, a base de dados do grupo farmacêutico reúne informações sensíveis de 48 milhões de pessoas, cerca de 20% da população

44 Disponível em: https://www.youtube.com/watch?v=fZao3vKAEEQ. Acesso em: 14 fev. 2024.

brasileira. Esses dados se referem ao histórico de saúde e ao comportamento sexual de 15 anos. "A sensibilidade desses dados está relacionada ao uso potencial para dar causa a discriminação proibida no ordenamento jurídico, em ofensa aos direitos fundamentais da liberdade e da igualdade assegurados na Constituição" (Ministério da Justiça e Segurança Pública, 2023), afirma o texto da notificação. Entre os questionamentos apresentados pela Senacon nessa notificação está a possível monetização dos dados dos clientes para propaganda de terceiros (Rossi, Amanda, 23 out. 2023).

5. Efetivação de direitos na economia de dados na saúde

O programa de fidelidade Stix é um bom exemplo do papel estratégico desempenhado pelo varejo farmacêutico na economia de dados, estabelecendo conexões entre farmácias, drogarias e empresas de diversos setores do varejo. Sob gestão do Stix Fidelidade e Inteligência S.A., essa iniciativa foi concebida por dois gigantes de mercado: a rede de farmácias Raia/Drogasil e o grupo GPA, um dos líderes do ramo alimentício na América do Sul, controlado pelo grupo francês Casino, que engloba marcas proeminentes como Pão de Açúcar e Extra.[45]

Além dos grupos fundadores, foram incorporados ao programa Stix as empresas Sodimac, Polishop, C&A e Magalu (*e-commerce* da loja de departamentos Magazine Luiza). Clientes Itaú e correntistas do Banco do Brasil, que participam do programa Livelo, também podem transferir pontos para o programa Stix.

O "*Ranking* das 300 maiores empresas do varejo brasileiro", editado pela Sociedade Brasileira de Varejo e Consumo (SBVC) em 2022[46], mostra a importância, o poder econômico e a capilaridade das empresas de varejo que estão conectadas ao programa Stix. As empresas fundadoras do programa de fidelidade atuam nos dois principais segmentos do varejo: supermercados e hipermercados (49,6%) e drogarias e perfumarias (12,4%); e as demais participantes ocupam posição de destaque no *ranking*.[47] Soma-se ao poder das empresas varejistas dois atores robustos do mercado financeiro, Itaú e Banco do Brasil, que estão entre os cinco bancos com maior número de clientes no país.

45 O programa unificou os sistemas de fidelidade desses grupos, permitindo que os consumidores acumulassem pontos Stix em suas compras em qualquer loja participante. Por exemplo, pontos obtidos em compras no Pão de Açúcar são somados aos ganhos na Drogaria Raia, podendo ser posteriormente utilizados para obter produtos e descontos em lojas parceiras.

46 Farta informação sobre o *ranking* está disponível em: https://sbvc.com.br/ranking-das-300-maiores-empresas-do-varejo-brasileiro/.

47 (**i**) O GPA, que reúne Pão de Açúcar e Extra, ocupa a 4ª colocação no segmento supermercados e hipermercados e 10º no geral. (**ii**) O grupo Raia/Drogasil é a 1ª no segmento drogarias e perfumarias e 6ª no geral. Além deles: (**iii**) Sodimac é a 3ª no segmento material de construção e 103ª no geral; (**iv**) Polishop ocupa o 5º lugar no segmento lojas de departamento e 84º no geral; (**v**) C&A é 3ª no segmento moda, calçados e artigos esportivos e 25ª do geral; (**vi**) Magazine Luiza ocupa o 1º no segmento lojas de departamento e o 3º no *ranking* geral.

A concentração de informações sobre as preferências e o comportamento do consumidor é de grande valor, pois permite a análise de tendências e a previsão de oportunidades de mercado, ao identificar potenciais interesses e necessidades dos clientes. Voltando ao exemplo das mulheres que compraram teste de gravidez, elas são potenciais compradoras de uma variedade de produtos, desde itens em farmácias e supermercados até materiais de construção, para preparar um quarto para o futuro bebê. Além disso, podem ter interesse em empréstimos bancários e consórcios. Essa compreensão ampla do comportamento do consumidor viabiliza estratégias de *marketing* mais eficazes, principalmente para quem tem acesso a dados diversificados, em grande volume e capacidade para processá-los.

A falta de transparência e informações ao consumidor quanto ao tratamento de seus dados pessoais para fins publicitários limita a participação desses usuários nas decisões sobre suas informações e sobre os anúncios que o atingem, alguns, inclusive, não desejados, especialmente considerando que a coleta de dados no setor farmacêutico é pulverizada e comporta um fluxo de informações potencialmente para outros agentes econômicos, do varejo e da indústria.

Tal situação revela que, do ponto de vista da afirmação de direitos, há um amplo conjunto de tópicos e organizações que podem ser mobilizados para proteção dos usuários. A transversalidade de temas comporta a defesa do consumidor, a proteção de dados pessoais, os aspectos do direito à saúde associados à não discriminação e o próprio acesso aos medicamentos.

Os diversos empregos econômicos identificados no uso de dados pessoais de saúde indicam que há grande interesse no tratamento desses dados, o que somado à falta de transparência demanda o aumento das estruturas de proteção para as pessoas.

O histórico dos casos indica que a efetivação desses direitos, particularmente no caso da proteção de dados pessoais, situa-se dentro do paradigma indicado por Coutinho (2008). Se por um lado, a própria aprovação da LGPD e o reconhecimento da proteção de dados como direito fundamental expresso na Constituição são frutos da mobilização da sociedade civil, por outro, nos indica que sua efetivação vem encontrando barreiras relacionadas a falta de enforcement das autoridades responsáveis pela efetivação desses direitos. O que vai ao encontro do sentimento de impotência dos usuários de saúde perante serviços cada vez mais digitalizados e assimétricos.

A despeito da aprovação de um extenso arcabouço legal que poderia ser mobilizado para resolver o problema, bem como de autoridades públicas constituídas para tal,

ainda existe sentimento de impotência das pessoas em relação ao uso de seus dados pessoais, bem como a impossibilidade de se abordar os dados de forma mais coletiva, pensando-se em estratégias para partilhar os benefícios da inovação com a sociedade.

A centralidade dos dados nos processos econômicos e as estratégias que tentam contornar a efetivação do direito à proteção de dados tornam essas disputas permanentes e assinalam um grande desafio para a sociedade civil e para os organismos do Estado.

São as contradições próprias da sociedade da informação, na qual os direitos digitais, e em particular a proteção de dados, que configuram a questão central da cidadania moderna da nossa época. A recorrência de casos de infração e a ampliação das estratégias de coleta de dados nas farmácias, e em outros ramos do varejo, indicam a necessidade de regulação mais específica e de fiscalização mais vigorosa.

Referências

ANPD. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. ANPD divulga nota técnica sobre tratamento de dados pessoais no setor farmacêutico. 12 maio 2023. **Ministério da Justiça e Segurança Pública**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-divulga-nota-tecnica-sobre-tratamento-de-dados-pessoais-no-setor-farmaceutico. Acesso em: 18 nov. 2023.

BATES, David W. *et al.* Big data in health care: using analytics to identify and manage high-risk and high-cost patients. **Health Affairs**, v. 33, n. 7, p. 1123-1131, 2014. DOI: 10.1377/hlthaff.2014.0041. Disponível em: https://pubmed.ncbi.nlm.nih.gov/25006137/. Acesso em: 18 nov. 2023.

BATISTA, Daiane. Tarcízio Silva: "O racismo algorítmico é uma espécie de atualização do racismo estrutural". **Centro de Estudos Estratégicos da Fiocruz Antonio Ivo de Carvalho**. 30 mar. 2023. Disponível em: https://cee.fiocruz.br/?q=Tarcizio-Silva-O-racismo-algoritmico-e-uma-especie-de-atualizacao-do-racismo-estrutural.

CESCR General Comment n. 14: The Right to the Highest Attainable Standard of Health (Art. 12) 2000. **Office of the High Commissioner for Human Rights**. Disponível em: https://www.ohchr.org/sites/default/files/Documents/Issues/Women/WRGS/Health/GC14.pdf. Acesso em: 18 nov. 2023.

COHN, Amélia. Caminhos da reforma sanitária. **Lua Nova: Revista de Cultura e Política**, v. 19, p. 123-140, nov. 1989. DOI: https://doi.org/10.1590/

S0102-64451989000400009. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.br/j/ln/a/q3sRL6qtG7NPGzmdMvtVVPz/?format=pdf&lang=pt. Acesso em: 18 nov. 2023.

COUTINHO, C. N. **Contra a corrente**: ensaios sobre democracia e socialismo. 2. ed. São Paulo: Cortez, 2008.

DAGENAIS, Simon *et al.* Use of real-world evidence to drive drug development strategy and inform clinical trial design. **Clinical Pharmacology & Therapeutics**, v. 111, n. 1, p. 77-89, jan. 2022. DOI: 10.1002/cpt.2480. Disponível em: https://pubmed.ncbi.nlm.nih.gov/34839524/. Acesso em: 18 nov. 2023.

FLEURY-TEIXEIRA Paulo. Uma introdução conceitual à determinação social da saúde. **Saúde em Debate**, 2009, v. 33, n. 83, p. 380-389. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.redalyc.org/pdf/4063/406345800005.pdf. Acesso em: 18 nov. 2023.

FORNAZIN, Marcelo; PENTEADO, Bruno Elias; CASTRO, Leonardo Costa de; CASTRO SILVA, Sandro Luís Freire de. From Medical Informatics to Digital Health: a Bibliometric Analysis of the Research Field. 9-13 ago. 2021. **AMCIS 2021 Proceedings**. 18. Disponível em: https://aisel.aisnet.org/amcis2021/healthcare_it/sig_health/18. Acesso em: 18 nov. 2023.

GOVERNO DE MATO GROSSO. Procon Estadual multa rede de farmácias por infração à Lei de Proteção de Dados Pessoais. 13 jul. 2021. **OGE**. Ouvidoria Geral do Estado. Notícias. Disponível em: https://www.ouvidoria.mt.gov.br/-/17504802-procon-estadual-multa-rede-de-farmacias-por-infracao-a-lei-de-protecao-de-dados-pessoais. Acesso em: 18 nov. 2023.

HSIAO, William C. What is a health system? Why should we care? **Harvard School of Public Health**, working paper, 33 p., ago. 2003. Disponível em:http://fpzg.hr/_download/repository/Hsiao2003.pdf. Acesso em: 18 nov. 2023.

IDEC. INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. Droga Raia e Drogasil desistem de pedir biometria para liberar descontos. 8 jul. 2021. Disponível em: https://idec.org.br/idec-na-imprensa/droga-raia-e-drogasil-desistem-de-pedir-biometria-para-liberar-descontos-0. Acesso em: 18 nov. 2023.

IDEC. INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. Pesquisa do Idec demonstra que preço teto dos medicamentos não impede reajustes abusivos. 27 mar. 2023. Disponível em: https://idec.org.br/release/pesquisa-do-idec-demonstra-que-preco-teto-dos-medicamentos-nao-impede-reajustes-abusivos. Acesso em: 15 fev. 2024.

IRIS. INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. Iris oferece representação ao MP-MG sobre prática de coleta de dados em redes de farmácias. 15 ago. 2018. Disponível em: https://irisbh.com.br/iris-oferece-representacao-ao-mp-mg-sobre-pratica-de-coleta-de-dados-em-redes-de-farmacias/. Acesso em: 18 nov. 2023.

IRIS. INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE. MPMG propõe medidas de adequação da prática de coleta do CPF em drogarias. 3 dez. 2018. Disponível em: https://irisbh.com.br/mpmg-propoe-medidas-de-adequacao-da-pratica-de-coleta-do-cpf-em-drogarias/. Acesso em: 18 nov. 2023.

KNOTH, Pedro. Exclusivo: Procon-SP fica insatisfeito com resposta da Drogasil sobre biometria. **Tecnoblog**, set. 2021. Disponível em: https://tecnoblog.net/noticias/2021/09/30/exclusivo-procon-sp-fica-insatisfeito-com-resposta-da-raia-drogasil-sobre-biometria/. Acesso em: 14 fev. 2024.

LONGUINHO, Daniella. Farmácias que pedem CPF para dar descontos serão investigadas pelo MJ. **RadioAgência**, 17 nov. 2021. Disponível em: https://agenciabrasil.ebc.com.br/radioagencia-nacional/justica/audio/2021-11/farmacias-que-pedem-cpf-para-dar-descontos-serao-investigadas-pelo-mj. Acesso em: 18 nov. 2023.

LUIZ, Gabriel. CPF em troca de desconto: MP investiga venda de dados de clientes por farmácias. **G1**, 16 mar. 2018. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/cpf-em-troca-de-desconto-mp-investiga-venda-de-dados-de-clientes-por-farmacias.ghtml. Acesso em: 18 nov. 2023.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (lei 13.709/2018) o novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, 2018, v. 120. Disponível em: https://www.academia.edu/42740879/Coment%C3%A1rio_%C3%A0_nova_Lei_de_Prote%C3%A7%C3%A3o_de_Dados_lei_13_709_2018_o_novo_paradigma_da_prote%C3%A7%C3%A3o_de_dados_no_brasil.

MINAS GERAIS. Ministério Público do Estado de Minas Gerais. TAC firmado com a Drogaria Araújo no âmbito da Investigação preliminar n. 0024.18.002027-3. Belo Horizonte, 18 set. 2018. Disponível em: https://drive.google.com/file/d/1kkV_NTw_E4OVRDLOwmT1_SWAe3F2aVmt/view. Acesso em: 14 fev. 2024.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Secretaria Nacional do Consumidor (Senacon). **Senacon notifica RaiaDrogasil sobre tratamento indevido de dados pessoais dos consumidores**. 23 out. 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/senacon-notifica-raiadrogasil-sobre-tratamento-indevido-de-dados-pessoais-dos-consumidores#:~:text=Bras%C3%ADlia%2C%2023%2F10%2F2023,dos%20

consumidores%2C%20relacionados%20%C3%A0%20sa%C3%BAde.
MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS. Investigação preliminar n. 0024.18.010995-1.

MINISTÉRIO PÚBLICO DO ESTADO DE MINAS GERAIS. Processo administrativo n. 0024.18.002027-3, do processo de fiscalização n. 00261.001371/2023-32, da Autoridade Nacional de Proteção de Dados.

MPDFT. MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. Inquérito civil público n. 08190.030923/19-55.

MIZIARA, Nathália Molleis. **Regulação do mercado de medicamentos**: a CMED e a política de controle de preços. Dissertação de Mestrado. São Paulo: Universidade de São Paulo, 2013. 229 p. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://teses.usp.br/teses/disponiveis/2/2133/tde-12022014-103446/publico/Nathalia_Miziara_Mestrado_VersaoFinal.pdf. Acesso em: 15 abr. 2024.

PANCH, Trishan; PEARSON-STUTTARD, Jonathan; GREAVES, Felix; ATUN, Rifat. Artificial Intelligence: opportunities and risks for public health. **The Lancet Digital Health**, v. 1, n. 1, p. e13-e14, maio 2019. DOI: https://doi.org/10.1016/S2589-7500(19)30002-0. Disponível em: https://www.thelancet.com/journals/landig/article/PIIS2589-7500(19)30002-0/fulltext. Acesso em: 15 abr. 2024.

PARANHOS, Julia; MERCADANTE, Eduardo; HASENCLEVER, Lia. Os esforços inovativos das grandes empresas farmacêuticas no Brasil: o que mudou nas duas últimas décadas? **Revista Brasileira de Inovação**, v. 19, p. e0200015, 2020. DOI: https://doi.org/10.20396/rbi.v19i0.8655780. Disponível em: https://periodicos.sbu.unicamp.br/ojs/index.php/rbi/article/view/8655780. Acesso em: 15 abr. 2024.

ROSSI, Amanda. Como ver o que a farmácia sabe sobre você e pedir para apagar os dados. **Portal Uol**, 1 set. 2023b. Disponível em: https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2023/09/01/como-ver-o-que-a-farmacia-sabe-sobre-voce-e-pedir-para-apagar-os-dados.htm. Acesso em: 15 fev. 2023.

ROSSI, Amanda. Farmácias: você dá o CPF, mas os descontos são reais? **Portal Uol,** 1 set. 2023a. Disponível em: https://noticias.uol.com.br/reportagens-especiais/farmacias-voce-da-o-cpf-mas-o-desconto-e-real/#cover. Acesso em: 15 fev. 2023.

ROSSI, Amanda. Ministério da Justiça notifica RaiaDrogasil após reportagem do UOL. **Portal Uol**, 23 out. 2023. Disponível em: https://economia.uol.com.br/noticias/redacao/2023/10/23/ministerio-da-justica-notifica-raiadrogasil-apos-reportagem-do-uol.htm. Acesso em: 26 abr. 2024.

ROSSI, Amanda. O que a farmácia sabe sobre mim? **Portal Uol**, 1 set. 2023c. Disponível em: https://noticias.uol.com.br/reportagens-especiais/o-que-a-farmacia-sabe-sobre-mim/. Acesso em: 15 fev. 2023.

ROSSI, Amanda. Vitamina usada para tentar engravidar pode direcionar até anúncio de carro. **Portal Uol**, 1 set. 2023d. Disponível em: https://noticias.uol.com.br/saude/ultimas-noticias/redacao/2023/09/01/remedio-para-engravidar-pode-direcionar-ate-propaganda-de-carro.htm. Acesso em: 15 fev. 2023.

SBVC. SOCIEDADE BRASILEIRA DE VAREJO E CONSUMO. *Ranking* das 300 maiores empresas do varejo brasileiro. 14 dez. 2022. Disponível em: https://sbvc.com.br/ranking-das-300-maiores-empresas-do-varejo-brasileiro/. Acesso em: 15 fev. 2023.

SILVA, Tarcízio. **Racismo Algorítmico: Inteligência Artificial e Discriminação nas Redes Digitais**. São Paulo: Edições SESC SP, fev. 2022. Disponível em: https://racismo-algoritmico.pubpub.org/.

SILVEIRA, Sergio Amadeu *et al.* A privacidade e o mercado de dados pessoais: Privacy and the market of personal data. **Liinc em Revista**, v. 12, n. 2, nov. 2016. DOI: 10.18617/liinc.v12i2.902. Disponível em: https://www.researchgate.net/publication/311878199_A_privacidade_e_o_mercado_de_dados_pessoais_Privacy_and_the_market_of_personal_data. Acesso em: 15 fev. 2023.

SOUZA, Caroline Miranda Alves de; PARANHOS, Julia; HASENCLEVER, Lia. Comparativo entre preço máximo ao consumidor de medicamentos e preços praticados na internet no Brasil: desalinhamentos e distorções regulatórias. **Ciência & Saúde Coletiva**, v. 26, n. 11, p. 5463-5480, nov. 2021. DOI: https://doi.org/10.1590/1413-812320212611.44082020. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.br/j/csc/a/VvSTxv8vqxbS76JDdCmbNLv/?format=pdf&lang=pt. Acesso em: 15 fev. 2023.

STEVANIM, Luiz Felipe; MURTINHO, Rodrigo. **Direito à comunicação e saúde**. Rio de Janeiro: Fiocruz, 2021.

WHO. WORLD HEALTH ORGANIZATION. Ethics and governance of artificial intelligence for health: guidance on large multi-modal models. 18 jan. 2024. Disponível em: https://www.who.int/publications/i/item/9789240084759. Acesso em: 15 mar. 2024.

WHO. WORLD HEALTH ORGANIZATION. Reducing health inequities through action on the social determinants of health. World Health Organization. World Health Assembly, 62. 2009. Disponível em: https://iris.who.int/handle/10665/2257. Acesso em: 15 mar. 2024.

https://doi.org/10.29397/EdicoesLivres/20250109

Governança de dados sobre a saúde como direito humano: uma proposta global

Angélica Baptista Silva
Vanessa de Lima e Souza

Um sintoma da sociedade da informação interconectada em rede refere-se aos registros que produzem dados sobre a saúde das pessoas. Esses dados circulam rapidamente e são objeto de financeirização, aumentando a brecha digital na saúde. No entanto, para a sobrevivência da humanidade, torna-se premente regular essa circulação, priorizando a vida e o bem-estar das pessoas.

A governança dos dados nos variados estabelecimentos de saúde pode ser uma potente resposta a esse desafio. Podemos defini-la como um conjunto de processos que envolvem a gestão da arquitetura institucional, a integração de sistemas, a colaboração e os agenciamentos, a responsabilização e a comunicação (Souza, 2018).

Nesse sentido, a Coalizão Transform Health é uma iniciativa internacional que está propondo em fóruns internacionais, como a Organização das Nações Unidas (ONU) e a Organização Mundial da Saúde (OMS), uma série de princípios para serem pactuados entre os governantes dos países.

Os princípios de Governança de Dados sobre a Saúde (GDSAS) foram conduzidos e desenvolvidos pela sociedade civil por um processo inclusivo e consultivo, administrado pela Coalizão Transform Health, entre 2020 e 2022. A formulação reuniu cerca de 200 colaboradores de mais de 130 organizações, em oito oficinas globais e regionais, e foi seguida de uma consulta pública mundialmente divulgada. Esse processo foi idealizado para reunir diferentes perspectivas e conhecimentos, e garantir o envolvimento de diversas partes interessadas de todas as geografias e setores, inclusive o Brasil.[48]

Este texto tem como objetivo apresentar a proposta global dos princípios de GDSAS das pessoas e fazer uma discussão desse tema no contexto brasileiro.

48 A Transform Health liderou esse processo, sob a coordenação de seu Círculo de Políticas, que inclui especialistas em saúde e governança de dados: Asia eHealth Information Network (AeHIN), FIND, Fondation Botnar, Grupo de Trabalho de Governança Digital e de Dados da Health Data Collaborative, I-DAIR, IT for Change, Jhpiego, PATH, Philips Foundation, Digital Connected Care Coalition (DCCC), Red Centroamericana de Informática en Salud (RECAINSA) e Young Experts: Tech 4 Health (YET4H). Os seguintes parceiros foram fundamentais para apoiar as consultas globais e regionais: PATH, AeHIN, BID Learning Network, Mwan Events, RECAINSA, Wilton Park, Governing Health Futures 2030 e YET4H. Esse trabalho foi financiado pela Fondation Botnar.

Os princípios de Governança de Dados Sobre a Saúde (GDSAS): universalizando os benefícios da digitalização da saúde

Os princípios de GDSAS trazem o olhar dos direitos humanos e da equidade para o uso de dados dentro dos sistemas de saúde e entre eles. Eles são orientados a apoiar sistemas de saúde pública sustentáveis e resilientes que possam oferecer a Universalidade da Cobertura no Acesso aos Serviços de Saúde (UCASS).[49]

Em 2019, na Reunião de Cúpula da ONU sobre a UCASS – termo equivalente a Universal Health Coverage (UHC) (Cobertura Universal de Saúde, em português) –, os líderes mundiais reafirmaram seu compromisso com os Objetivos de Desenvolvimento Sustentável (ODS) de estender a UCASS a todas as pessoas até 2030. A saúde digital e os sistemas de saúde orientados por dados podem ajudar a fortalecer a oferta, a qualidade e a equidade de serviços de saúde, proporcionando oportunidades para acelerar o progresso em direção à universalidade nos serviços de saúde. A UCASS – e os valores de equidade e de direitos humanos que a sustentam – deve estar no cerne da concepção e do desenvolvimento de sistemas de saúde orientados por dados.

As abordagens orientadas por dados são cada vez mais frequentes no funcionamento dos sistemas de saúde e na prestação de serviços de saúde. A coleta, o processamento, o armazenamento, a análise, o uso, o compartilhamento e o descarte de dados sobre a saúde têm crescido em complexidade. A pandemia de covid-19 acelerou o uso de dados. Esse aumento exponencial no uso exige uma governança robusta e equitativa dos dados sobre a saúde. Países e regiões, ao redor do mundo, estão instituindo políticas e legislações de GDSAS. No entanto, não existe ainda um conjunto global e abrangente de princípios para orientar essa governança nos sistemas e nas políticas de saúde pública. Os princípios de GDSAS surgem como uma resposta a essa necessidade.

Os princípios de GDSAS objetivam informar e fortalecer modelos de governança, instrumentos, tratados, regulamentos e padrões entre países e regiões em torno de uma visão compartilhada de governança equitativa. Eles são uma ferramenta para apoiar o uso de tecnologias e dados digitais para a saúde e o bem-estar de todos, um avanço necessário para uma estrutura global de GDSAS.

49 A lei de n. 8.080, de 19 de setembro de 1990, no capítulo II, menciona como um dos princípios doutrinários do Sistema Único de Saúde (SUS) a "universalidade de acesso aos serviços de saúde em todos os níveis de assistência", que é equivalente ao termo usado pela OMS e pela ONU – Cobertura Universal de Saúde (tradução nossa), em um sistema nacional de saúde (Brasil, 1990).

Os princípios são construídos e reconhecidos mediante normas, tratados, convenções e diretrizes existentes, incluindo: "Princípios de dados da OMS" (WHO, 2020); "Ética e governança da Inteligência Artificial (IA) para a saúde: orientação da OMS" (WHO, 2021); "Princípios para o desenvolvimento digital" (The Digital Impact Alliance, 2017); "Princípios de investimento digital" (The Digital Impact Alliance, 2018); "Recomendação do conselho sobre governança de dados de saúde" (OECD/LEGAL/0433, 2023); "Recomendação do conselho sobre Inteligência Artificial" (OECD/LEGAL/0449, 2019); "8 princípios orientadores da transformação digital do setor da saúde" (OPAS, 2021); relatórios da *The Lancet* e da *Financial Times Commission on governing health futures 2023* (Kickbusch *et al*., 2021); "Declaração Universal dos Direitos Humanos" (ONU, 1995); "Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais" (Brasil, 1992a); "Pacto Internacional sobre Direitos Civis e Políticos" (Brasil, 1992b); e "Princípios de Siracusa sobre a limitação e derrogação de disposições do Pacto Internacional sobre Direitos Civis e Políticos" – sendo os três últimos ratificados por decretos no Brasil. Os princípios de GDSAS são baseados nesses esforços, enquanto fortalecem ainda mais o ecossistema de Governança de Dados sobre a Saúde.

Objetivos

Os princípios estão agregados em torno de três objetivos interconectados:

(1) proteger as pessoas – como pessoas, como grupos e como comunidades;
(2) promover o valor da saúde – por meio do compartilhamento de dados e de usos inovadores de dados;
(3) priorizar a equidade – garantindo a distribuição equitativa dos benefícios decorrentes do uso de dados nos sistemas de saúde.

Sobre proteger as pessoas, defende-se que a GDSAS garanta a proteção de pessoas, grupos e comunidades contra danos e violações relacionados aos dados. A proteção de pessoas é, muitas vezes, incorporada em leis gerais de proteção de dados. No entanto, devido à sua natureza potencialmente sensível, os dados sobre a saúde requerem proteções especializadas adicionais na lei e nas práticas de tratamento desses dados. Dados desprotegidos (pessoais e agregados) sobre a saúde podem expor pessoas, grupos e comunidades a danos. A GDSAS deve

incluir medidas especiais de proteção contra vários tipos de danos individuais e coletivos, incluindo exploração orientada por dados, assédio, discriminação, capitalismo de vigilância[50] e neocolonialismo.[51]

Quanto a promover o valor da saúde, propõe-se que a GDSAS deve maximizar o valor obtido pelo uso e pela análise de dados para melhorar os resultados no setor de saúde, tanto para as pessoas, quanto para a sociedade. Muitas vezes, isso requer que algumas formas de dados sejam amplamente compartilhadas, pois os dados isolados podem levar a uma compreensão insuficiente do valor da saúde. A agregação e o compartilhamento de dados sobre a saúde devem ser feitos de forma a proteger os direitos individuais, grupais e comunitários. Além disso, como as abordagens baseadas em dados podem levar a novos tipos de serviços de saúde, a GDSAS deve apoiar e promover tais inovações.

O último objetivo diz respeito a priorizar a equidade. Assim, o valor da saúde criado pelo uso de dados deve beneficiar igualmente as pessoas e as comunidades. Os dados são constituídos de pessoas, seja como cidadãos ou como comunidades, e, portanto, as pessoas devem ter uma participação equitativa no valor da saúde originado de seus dados.

A maioria das abordagens atuais de governança de dados adota uma visão individualista, e não baseada na solidariedade que maximize a importância dos dados sobre a saúde para todas as populações. Os princípios da GDSAS equilibram as perspectivas individuais e coletivas dentro de cada um dos três objetivos. Proteger as pessoas considera a importância da proteção de dados de grupos e de comunidades. Promover o valor da saúde aborda as necessidades e os benefícios coletivos dos sistemas de saúde pública. Priorizar a equidade requer equidade entre grupos e pessoas.

Os princípios destinam-se a ser uma ferramenta e são aplicáveis aos vários envolvidos na GDSAS, incluindo: governos, parlamentares e formuladores de políticas; organizações internacionais, iniciativas globais de saúde e bancos de desenvolvimento; o setor privado; organizações sem fins lucrativos e não governamentais; instituições acadêmicas e de pesquisa; doadores e fundações; sociedade civil (incluindo grupos ativistas, organizações de pacientes etc.); coalizões globais; administradores de dados e usuários; e o próprio público.

---

50 De acordo com Shoshana Zuboff (2021), cunhadora da expressão capitalismo de vigilância, trata-se de uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas; uma expropriação de direitos humanos fundamentais que pode ser mais bem compreendida como um golpe vindo de cima: uma destituição da soberania dos indivíduos.

51 Para Kwame Nkrumah (1965), o neocolonialismo representa o imperialismo em seu estágio final e mais perigoso. Sua essência é de que o Estado é, em teoria, independente e tem toda as aparências exteriores da soberania internacional, todavia, seus sistemas econômico e político são geridos no exterior, por empresas.

Os oito princípios da GDSAS

Os oito princípios da GDSAS procuram unir interessados em torno de elementos centrais que o descrevam melhor e expressem como esses princípios podem ser colocados em prática. Estão destinados a promover a governança equitativa dos dados sobre a saúde, criando uma visão comum e um ambiente no qual todos possam compartilhar, usar e se beneficiar dos dados sobre saúde. São projetados para complementar e reforçar um ao outro, sendo apresentados sem ordem de prioridade.

1. Princípio I – Proteger pessoas e comunidades

A GDSAS deve proteger pessoas, grupos e comunidades contra danos e violações em todas as fases do ciclo de vida dos dados.[52] A governança de dados deve buscar o equilíbrio entre a proteção e os direitos de pessoas, grupos e comunidades com o valor social do uso de dados para a saúde. Esse equilíbrio requer análise rigorosa e avaliação de risco das práticas de dados para identificar e mitigar possíveis danos, que devem ser incorporados em todas as etapas desse ciclo. Da mesma forma, requer uma participação significativa da sociedade civil, das comunidades e pessoas. Seus elementos centrais estão detalhados a seguir.

1.1 Abordar e prever o risco individual e coletivo

A GDSAS deve priorizar a redução do risco individual e coletivo, seguindo a doutrina de "não causar dano". A coleta e o uso de dados sobre a saúde devem mitigar os riscos potenciais que as pessoas possam enfrentar. Esses riscos variam de moderados (como a perda de privacidade de dados) a riscos graves (como riscos à segurança pessoal, riscos de cuidados insuficientes ou incorretos, ou mesmo exploração). Quando os dados são anonimizados, a GDSAS deve mitigar os riscos coletivos, incluindo aqueles relacionados a um grupo ou a uma comunidade específicos (riscos de discriminação) e aqueles relacionados à sociedade em geral (riscos à saúde pública).

1.2 Coletar dados com propósitos definidos

As necessidades específicas de dados devem ser claramente definidas antes de qualquer coleta. Os coletores e administradores de dados devem comunicar essas necessidades às pessoas e às comunidades que os fornecem. A GDSAS

52 No Transform Health, o "ciclo de vida dos dados" é referido como o conjunto das etapas de coleta, processamento, armazenamento, análise, uso, compartilhamento e descarte dos dados.

deve incluir diretrizes sobre as necessidades e as limitações da coleta de dados (exemplo: coletar apenas os dados necessários e usar os existentes).

1.3 Coletar dados pessoais ou sensíveis somente quando necessário e com consentimento informado

Dados pessoais ou sensíveis sobre a saúde devem ser coletados somente quando necessário para alcançar um objetivo específico e justificável de saúde, advindo de pesquisa ou para uma política (exemplo: registros eletrônicos de saúde podem incluir dados sensíveis necessários para melhorar o cuidado do paciente). Nesse sentido, as políticas, leis e regulamentações relativas à GDSAS devem seguir os padrões globais e as melhores práticas.

Os coletores e administradores de dados devem obter o consentimento informado antes que os dados sejam coletados. O consentimento informado exige a compreensão completa por parte das pessoas de seus direitos e de que forma seus dados de saúde podem ser usados. Quando as situações exigem isenções para esse requisito (exemplo: emergências de saúde pública), essas devem ser legais, justificadas e limitadas à circunstância específica.

1.4 Utilizar mecanismos seguros de coleta e armazenamento de dados

A proteção de dados sobre a saúde requer métodos seguros de coleta de dados (exemplo: uso de ferramentas de coleta com funcionalidade robusta de proteção de dados) e de armazenamento seguro de dados (exemplo: criptografia, servidores em nuvem). Deve-se considerar o tempo de armazenamento, com orientação sobre um prazo razoável, após o qual os dados devem ser excluídos ou removidos do sistema (exemplo: cláusulas de caducidade). Como os dados pessoais de saúde são dados "para toda a vida", as políticas de retenção de dados relacionadas aos registros de atendimento não devem criar lacunas nos registros longitudinais de saúde. Políticas abrangentes de segurança de dados também devem responder às abordagens de transferência de dados (exemplo: unidades USB, discos rígidos externos, roteadores, servidores, bases de dados) e ao ecossistema de inovação em saúde em evolução.

1.5 Utilizar desidentificação/pseudonimização e anonimização

A GDSAS deve definir o nível e a extensão da proteção de privacidade a que uma pessoa tem direito e os mecanismos associados para garanti-la. Para cada estágio do ciclo de vida dos dados, a GDSAS deve indicar onde a desidentificação e a

anonimização são necessárias para a proteção individual e comunitária. Além disso, a GDSAS deve delinear a proteção para dados pseudonimizados e anonimizados, pois esses dados podem expor informações confidenciais. A possibilidade de reidentificação, resultante de rápidos desenvolvimentos tecnológicos, também deve ser considerada (exemplo: por algoritmos de análise de dados ou triangulação de fontes de dados).

1.6 Definir usos inadequados de dados sobre a saúde

A GDSAS deve abordar especificamente a coleta ou o uso ilegal, inadequado e antiético de dados sobre a saúde. Isso pode incluir vigilância não relacionada à saúde pelo Estado ou por outros atores, ou discriminação e assédio por entidades públicas ou privadas, especialmente contra grupos e populações marginalizadas. Modelos de governança nacional e global, relevantes para a era digital, são necessários para defender os direitos humanos fundamentais em todo o ciclo de vida dos dados sobre a saúde.

1.7 Instituir mecanismos de proteção contra discriminação, estigma, assédio e preconceito

A GDSAS deve instituir e fortalecer mecanismos e processos para abordar e prevenir a discriminação social, o estigma, o assédio e o preconceito, como um componente necessário da concepção do sistema de saúde com auditorias regulares. A GDSAS deve considerar o contexto cultural no qual é aplicada. O treinamento, a educação permanente dos profissionais de saúde e o engajamento significativo de diversas comunidades podem ajudar a mitigar a discriminação, o estigma, o assédio e o preconceito.

1.8 Fornecer orientação específica para grupos e populações marginalizadas

As práticas de GDSAS devem responder aos contextos únicos e às necessidades relacionadas aos dados, bem como aos possíveis danos relacionados aos dados de grupos e de populações marginalizadas. Práticas que podem parecer inofensivas para a população em geral podem trazer perigos específicos relacionados a certos grupos e a certas comunidades, como os de maior risco de HIV (exemplo: profissionais do sexo, usuários de drogas injetáveis, trabalhadores informais, pessoas transgênero).

Diretrizes relevantes devem afirmar a importância não apenas ao reconhecer os contextos únicos de populações vulneráveis, mas ao efetivar também a inclusão

significativa de tais grupos na formulação de princípios de governança de forma mais geral. As recomendações existentes e as outras orientações específicas para os marginalizados devem ser incorporadas às políticas e aos processos de GDSAS. O Fundo das Nações Unidas para a Infância (Unicef, 2021) produziu um manifesto sobre a melhor governança de dados das crianças.

2. Princípio II – Construir confiança nos sistemas de dados

Uma GDSAS bem desenvolvida deve reforçar a confiança nos sistemas e nas práticas de dados. O desenvolvimento de sistemas de GDSAS de maneira participativa e transparente, bem como a garantia de que os regulamentos e as diretrizes sejam acessíveis, compreendidos e seguidos, na prática, podem ajudar a criar confiança. A confiança requer a proteção dos dados, a preservação da privacidade e o estabelecimento de processos transparentes e inclusivos em todo o ciclo de vida dos dados. Também exige a capacidade de resposta às perguntas dos titulares dos dados e dos outros interessados e os mecanismos para lidar com reclamações. A seguir, tratamos um pouco dos elementos centrais que compõem o princípio II.

2.1 Alinhar-se com as práticas recomendadas de proteção e privacidade de dados

A GDSAS deve aplicar as práticas recomendadas existentes – e estabelecer novas – para proteger dados individuais e coletivos. Isso inclui abordagens técnicas para coleta e armazenamento de dados (exemplo: autenticação de dois fatores, criptografia, desidentificação) e políticas e processos relacionados ao acesso e uso dos dados (exemplo: políticas de segurança, permissões do sistema).

A GDSAS deve se alinhar e aprender com políticas e regulamentos bem estabelecidos, tais como: o Regulamento Geral sobre a Proteção de Dados na Europa (RGPD) (General Data Protection Regulation) (GDPR, *s.d.*); a Lei de Proteção de Dados Pessoais (PDPA) em Singapura (PDPC | PDPA Overview, *s.d.*); a Lei de Proteção de Informações Pessoais na África do Sul (Protection of Personal Information Act (POPI Act, *s.d.*); e a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil (Brasil, 2018).

2.2 Garantir que o consentimento seja informado e compreendido em todas as suas complexidades

Ao coletar os dados de uma pessoa, o titular dos dados deve entender quais dados são coletados e o porquê, seus direitos em relação ao acesso, formas de alteração

ou remoção do sistema, como seus dados informam os cuidados pessoais e se estes podem ser reutilizados para fins adicionais. As pessoas também devem ter uma opção razoável de aceitar ou recusar a coleta de dados ou o compartilhamento adicional para outros fins que não o uso pretendido inicial, além de poder retirar o seu consentimento. O consentimento informado deve ser articulado de forma clara (inclusive, no idioma local) para garantir a acessibilidade àqueles que não estão familiarizados com a linguagem técnica ou jurídica.

O consentimento informado é o padrão-ouro para a GDSAS. No entanto, as políticas e os processos de GDSAS devem reconhecer a complexa realidade do consentimento informado, particularmente para os grupos e as populações marginalizadas. Uma pessoa pode ser solicitada a fornecer seus dados para receber serviços de saúde e, portanto, pode se sentir compelida a consentir, independentemente de sua compreensão ou concordância sobre como os dados serão usados. Em todas as instâncias, a proteção e o agenciamento informado de uma pessoa ou comunidade devem ser levados na mais alta consideração. A GDSAS deve, portanto, articular uma visão diferenciada do consentimento, considerando as circunstâncias, a gama de opções realistas e as relações de poder em uma dada situação.

2.3 Obter consentimento coletivo quando apropriado

Os dados sobre a saúde podem estar relacionados a uma característica específica de comunidade ou grupo (exemplo: pacientes com uma doença rara, grupos vulneráveis a uma doença específica). Isso tanto defende os direitos coletivos, quanto serve para construir e manter a confiança.

2.4 Definir exceções concretas ao consentimento informado

Políticas e processos de GDSAS devem definir de forma clara e transparente as circunstâncias em que são permitidas exceções ao consentimento informado. Exceções devem ser limitadas às situações em que uma intervenção para salvar a vida requer a autorização de um responsável legal, em que os requisitos do consentimento individual representam uma barreira aguda à saúde pública (exemplo: emergências de saúde pública); quando há um requisito legal legítimo e justificável; ou quando os dados são processados ou compartilhados de forma agregada (exemplo: dados de nível populacional). As exceções devem ser legais, necessárias e proporcionais, evitando o uso indevido para prejudicar ou explorar uma pessoa, um grupo ou uma comunidade.

2.5 Garantir a qualidade, a disponibilidade e a acessibilidade dos dados

A confiança nos sistemas de dados também requer confiança na qualidade dos dados. A GDSAS deve promover a melhoria geral da qualidade dos dados e torná-los mais disponíveis e acessíveis, conforme apropriado. Padrões globais devem ser adotados e adaptados aos contextos regionais, nacionais e locais, para promover a coleta de dados precisa, confiável e de alta qualidade.

2.6 Reforçar a GDSAS com evidências

A GDSAS deve ser fundamentada por evidências de seu uso e impacto, positivos ou negativos, com avaliação periódica em relação às melhores práticas, contribuindo para sua evolução contínua. Quando são identificadas lacunas nas práticas e/ou nos conhecimentos existentes, esforços devem ser feitos para identificá-las. Dessa forma, se estará contribuindo para a base de evidências global relacionada à GDSAS. Isso inclui as interações regulares e o aprendizado, a partir de estruturas de saúde digital globais e nacionais.

2.7 Estabelecer processos e sistemas transparentes e acessíveis

A transparência na GDSAS pode gerar adesão dos interessados em relação aos processos de dados, permitindo uma melhor reutilização de dados, maior colaboração em metodologias de análise de dados e percepção de melhor qualidade dos dados. A Data Futures Partnership (New Zeland Government, *s.d.*), na Nova Zelândia, define o uso transparente de dados com três dimensões: valor, proteção e escolha. Todos os envolvidos devem entender como e por que os dados são coletados (valor); como os dados são armazenados, analisados e usados (proteção); e como operam os sistemas e processos que suportam a GDSAS (escolha).

A transparência é essencial para os setores público e privado. Enquanto que as políticas públicas de dados, de IA e de tecnologias emergentes devem ser de acesso aberto, participativas e centradas nas pessoas. Os serviços do setor privado, como a telemedicina, devem construir a confiança nos pacientes, reconhecendo os contextos, os idiomas e as aplicações locais.

2.8 Instituir mecanismos de retorno e de responsabilização institucionais

A GDSAS inclusiva, equitativa e responsável requer mecanismos nos quais pessoas e comunidades possam: relatar o uso indevido de dados, fazer consultas sobre as estruturas e os processos dos dados sobre a saúde, solicitar a remoção de dados do sistema e receber retorno das suas solicitações. Esses processos devem ser apoiados por mecanismos como auditoria de dados estatutária e supervisão

independente. Os fornecedores de dados devem ser informados proativamente sobre seu direito ao retorno e receber benefícios decorrentes do compartilhamento e uso de dados.

3. Princípio III – Garantir a segurança dos dados

A segurança de dados é um componente essencial da GDSAS, abrange requisitos técnicos e processuais para a proteção de pessoas e comunidades. Isso inclui a aplicação de melhores práticas no ciclo de vida dos dados. Esse princípio é relevante para além do setor de saúde. As melhores práticas relacionadas à segurança devem evoluir continuamente à medida que novas tecnologias são introduzidas. Elencamos os elementos centrais desse princípio na sequência.

3.1 Exigir medidas de segurança técnica rígidas para o processamento de dados

Qualquer processo técnico aplicado para coletar, processar, armazenar, utilizar ou compartilhar dados deve empregar mecanismos de segurança robustos, sobretudo, quando da concepção de tecnologias e processos para fomentar a confiança – para esse fim é necessário definir diretrizes restritivas. Isso pode incluir requisitos de senha, autenticação de dois fatores, chaves de segurança e criptografia de dados. As instalações de armazenamento e processamento de dados devem ser protegidas, a partir de padrões de segurança globais ou nacionais. Além disso, a GDSAS deve abordar riscos comuns de segurança, incluindo *phishing* e vírus. As auditorias de segurança de dados devem ser periódicas.

3.2 Mitigar riscos relacionados às ameaças de segurança

A GDSAS deve considerar como minimizar o impacto de possíveis violações de segurança em pessoas, comunidades e sistemas de saúde. Isso pode incluir: o uso de identificadores unívocos, substituindo o nome da pessoa; a implementação de limites temporais de armazenamento; a inserção de medidas de segurança aprimoradas para os dados de identificação pessoal ou para outros dados sensíveis; as iniciativas para garantia da segurança cibernética; as diretrizes de armazenamento seguro para dados confidenciais; e os esforços para respeitar, proteger e defender o direito à privacidade como um princípio de concepção do sistema.

3.3 Garantir a transparência em relação a violações de dados

Quando ocorrem violações de dados, a GDSAS deve exigir que as partes informem às pessoas e às comunidades afetadas, bem como reportem a violação aos órgãos

reguladores envolvidos. Devem ser fornecidas informações sobre a natureza da violação, quais dados foram expostos e ações específicas devem ser tomadas para evitar outro evento futuro. Cada violação significativa deve ser revisada por mecanismos de supervisão independentes.

3.4 Considerar os sistemas de dados federados

A segurança, os direitos e a propriedade dos dados podem ser aprimorados por meio do armazenamento federado, processamento e uso de dados. Os sistemas de dados federados permitem que eles permaneçam próximos de seu ponto de origem (exemplo: na unidade de saúde em questão), enquanto ainda permitem a visualização e a análise baseadas em consentimento em todo o sistema de saúde. Eles reúnem várias fontes de dados autônomas para permitir o compartilhamento e o aprendizado entre sistemas, enquanto se adaptam às boas práticas de dados, através de diversos setores. Essa abordagem pode maximizar a utilidade e o uso dos dados e criar novas oportunidades para gerar contribuições de vários intervenientes em todos os setores.

4. Princípio IV – Melhorar os sistemas e os serviços de saúde

A GDSAS deve permitir o uso significativo de dados para melhorar a eficiência e a resiliência do sistema de saúde, aumentar o acesso à saúde e promover a equidade em saúde, para alcançar a UCASS. Uma abordagem para todo o sistema de saúde deve ser aplicada, garantindo que a GDSAS apoie a transformação dos sistemas de saúde. Os benefícios de uma boa GDSAS devem incluir totalmente as pessoas e as comunidades, que partilham seus dados. Os elementos centrais do princípio IV estão apresentados a seguir.

4.1 Avaliar os benefícios dos dados sobre a saúde

Além de melhorar o acesso aos serviços de saúde, os dados sobre a saúde oferecem oportunidades para uma maior qualidade, eficiência, eficácia e sustentabilidade dos sistemas de saúde. O uso de dados também cria oportunidades de inovação e avanços nas ciências médicas. O valor proporcionado por esses avanços deve ser considerado na definição do uso potencial dos dados sobre a saúde. Os interessados (exemplo: instituições de pesquisa ou academia) podem exigir legitimamente o acesso apropriado e seguro aos dados, porém, as pessoas e as comunidades também devem entender como seus dados podem auxiliar a pesquisa e o desenvolvimento.

4.2 Usar dados para aprimorar os serviços de saúde para pessoas e comunidades

A GDSAS deve aprimorar a utilização dos dados sobre a saúde para melhorar a saúde e o bem-estar, inclusive de pessoas e de comunidades que os forneceram. Isso pode ser feito de várias maneiras, por exemplo, pode-se: aprimorar o acesso aos serviços de saúde, fortalecer a vigilância, melhorar diagnósticos e análises preditivas na medicina de precisão etc. Melhorar o atendimento individual e garantir a segurança do paciente requer o compartilhamento de dados entre as unidades de saúde e os profissionais de saúde para apoiar um atendimento contínuo. O compartilhamento de dados também é necessário para apoiar a informática em saúde pública e as ações baseadas em dados. Políticas de compartilhamento e acesso devem ser elaboradas antes da permissão do uso de dados.

4.3 Incentivar uma cultura de ideias e ações baseadas em dados

Os dados sobre a saúde agregam valor significativo aos sistemas e serviços de saúde, possibilitando melhorias na saúde pública e na vida das pessoas. A GDSAS deve incentivar uma cultura que explore, desenvolva e use ideias baseadas em dados em todos os níveis de um sistema de saúde para abordar as desigualdades em saúde e aprimorar os serviços de saúde. A GDSAS deve ser projetada de forma a conquistar a confiança dos usuários dos dados e dos tomadores de decisão, para que os dados usados sejam de alta qualidade, e para que o manejo seja feito de forma legal e ética.

4.4 Abordar a eficiência, a eficácia e a resiliência do sistema de saúde

A governança apropriada dos dados sobre a saúde é um pré-requisito para um sistema de saúde resiliente e responsivo e que pode melhorar a eficiência e a eficácia dos serviços de saúde. Esses benefícios podem se estender a todos os componentes operacionais de um sistema de saúde (exemplo: cadeia de suprimentos, gestão da força de trabalho em saúde). A GDSAS deve incluir melhorias operacionais ao definir as necessidades de dados.

4.5 Fortalecer a propriedade comunitária de dados sobre a saúde

Os sistemas de dados centralizados concentram a tomada de decisão e o poder. Os sistemas de dados sobre a saúde devem ser projetados e operados de forma a aumentar a autonomia, o gerenciamento e a tomada de decisão em nível comunitário relacionados à coleta e ao uso de dados sobre a saúde.

4.6 Capacitar e empoderar os profissionais de saúde da linha de frente

A GDSAS deve revelar e potencializar o papel essencial, o valor e o trabalho dos profissionais de saúde da linha de frente, que devem ser centrais na concepção de sistemas de saúde orientados por dados. Deve haver um esforço intencional para garantir que a tomada de decisões baseada em dados seja fortalecida pelo uso de sugestões vindas do trabalho diário desses profissionais, sem enfraquecer o papel deles. Deve ser oferecido a esses trabalhadores oportunidades de desenvolvimento contínuo de habilidades e outros recursos de apoio à coleta e ao uso de dados sobre a saúde. Eles devem estar envolvidos no projeto, no desenvolvimento e na melhoria contínua de sistemas orientados por dados.

5. Princípio V – Promover o compartilhamento e a interoperabilidade

O compartilhamento de dados é um pré-requisito para criar valor, a partir de dados sobre a saúde, mas deve ser feito de forma a apoiar a equidade e os direitos humanos. Nos níveis regional, nacional e global, o compartilhamento de dados permite sugestões mais significativas acerca das necessidades e dos desafios de saúde, incluindo a prevenção e as respostas às emergências de saúde. Sistemas projetados para interoperabilidade (exemplo: em torno de protocolos, estruturas e definições comuns) permitem o compartilhamento e garantem a qualidade dos dados. A seguir, destacamos os elementos centrais da promoção do compartilhamento e da interoperabilidade.

5.1 Estabelecer regras e diretrizes de compartilhamento de dados

A GDSAS deve incluir regras e diretrizes que abordem uma variedade de cenários. Isso inclui o compartilhamento de dados necessários para a prestação de cuidados individuais entre agências públicas dentro de um país, entre sistemas governamentais e setor privado, dentro do setor privado e entre partes envolvidas – regionais, nacionais e globais.

As políticas de compartilhamento de dados devem minimizar o risco individual e coletivo, enquanto melhoram a equidade em saúde pública. Aproveitar o compartilhamento para usar dados coletados anteriormente pode até reduzir a necessidade e a extensão de nova coleta.

5.2 Validar o consentimento informado antes de compartilhar os dados

Os dados devem ser usados apenas para a finalidade para a qual foram coletados, exceto se o consentimento informado para usos subsequentes já tenha sido

fornecido pelo proprietário dos dados. Se acordos claros de compartilhamento de dados não estiverem em vigor, antes da coleta, um consentimento adicional pode ser exigido daqueles que originalmente contribuíram com os dados.

5.3 Promover a interoperabilidade dos sistemas de dados

Os dados e os sistemas digitais de saúde que apoiam a coleta e o uso devem ser concebidos tendo em mente a interoperabilidade. Essa interoperabilidade tornará o compartilhamento de dados entre sistemas mais simples e seguro, evitando possíveis erros durante as transferências manuais. A interoperabilidade é alcançada através da aplicação de padrões reconhecidos (exemplo: campos de dados básicos) e do desenho do sistema (exemplo: uso de interfaces, de API de programação de aplicativos abertos). Conceitos como portabilidade de dados, dados abertos, dados de comunidade, administração e trocas de dados também podem ser considerados como parte desses mecanismos.

5.4 Definir estruturas de dados comuns entre sistemas de saúde

Estruturas de dados comuns (exemplo: campos específicos para coleta de dados, arquitetura subjacente dos sistemas de dados) apoiarão o compartilhamento de dados, bem como o uso de tecnologias emergentes, permitindo previsibilidade e consolidação mais fáceis, a partir de diversos sistemas de dados. Essas estruturas permitem interoperabilidade e oportunidades para compreensões mais complexas que agregam valor e eficiência às ciências médicas e melhoram os resultados para o setor de saúde, além de fornecer garantias quanto aos tipos de dados disponíveis para uso futuro.

5.5 Definir vários níveis de acesso aos dados

A GDSAS deve identificar os tipos de acesso que cada envolvido deverá ter aos vários níveis de dados (incluindo os não identificados ou anonimizados), com o objetivo de reduzir o risco de exposição, sem prejudicar a geração de valor adicional.

Essas permissões podem existir em um nível técnico (exemplo: permissões de sistemas) e/ou organizadas, por meio de instituições, como autorizações de uso de dados, que definem claramente direitos, papéis e responsabilidades de diferentes atores.

5.6 Utilizar definições comuns e padrões globais

A GDSAS deve utilizar a terminologia e as definições dos principais conceitos existentes, como tipos de dados, protocolos do sistema e funções e responsabilidades

das partes interessadas. Tais definições são fornecidas por órgãos normativos globais e amplamente utilizadas nos setores públicos e privados. Os padrões e as estruturas de dados existentes, incluindo a norma ISO/TS 22220:2011 (ISO, 2011, p. 22220), o Fast Healthcare Interoperability Resources do HL7 (Health Level 7, *s.d.*), o OpenHIE da Health Information Exchange (OpenHIE, *s.d.*), a empresa inventora do código de barras, GS1 (2024), e outros, devem ser aplicados sempre que possível. Isso promove maior padronização e comparabilidade dos dados sobre a saúde, o que permite maior interoperabilidade entre sistemas, compartilhamento, qualidade e limpeza dos dados.

5.7 Apoiar parcerias multissetoriais

A GDSAS deve apoiar parcerias entre governos nacionais, setor privado, instituições acadêmicas, sociedade civil, organizações não governamentais e outros interessados, para criar um ecossistema seguro, robusto e resiliente no ciclo de vida dos dados. São necessárias políticas claras para construir relações de confiança e parcerias que devem priorizar os interesses de pessoas e comunidades, que fornecem os dados, e os interesses sociais mais amplos, especialmente de equidade em saúde pública.

6. Princípio VI – Facilitar a inovação usando os dados sobre a saúde

A GDSAS deve ser voltada para o futuro e antecipar a aplicação de tecnologias emergentes, como a IA. O aproveitamento da evolução contínua das tecnologias digitais e dos sistemas de dados é algo fundamental para alcançar os ODS e a UCASS. Isso requer desenvolver um ambiente de governança que pode acomodar e possibilitar a inovação de forma flexível, sendo a governança efetivamente aplicada às novas tecnologias e aos tipos de uso de dados. Os elementos centrais do princípio VI são comentados a seguir.

6.1 Aplicar a GDSAS às tecnologias emergentes

As tecnologias emergentes não podem ser isentas de verificações e restrições instituídas pela GDSAS. Novas tecnologias digitais devem considerar princípios, políticas e legislação de GDSAS, desde os estágios de concepção e *design*. Mecanismos devem ser definidos para abordar potenciais conflitos entre a GDSAS existente e as necessidades das tecnologias. As facilidades de "caixas de areia" para testes controlados direcionadas às inovações técnicas e de negócios podem ser úteis nesse sentido. Diante do rápido desenvolvimento tecnológico, podem

ser necessárias diretrizes gerais, além de normas específicas que se referem a contextos tecnológicos atuais e conhecidos, por exemplo, guia sobre ética e governança da IA na saúde, da OMS (WHO, 2021).

6.2 Abordar o uso de dados não relacionados à saúde em contextos de saúde

Muitas tecnologias e práticas de saúde digital utilizam dados de fontes, além dos sistemas de saúde. A GDSAS deve considerar outros tipos de fontes de dados que podem ser combinados com os dados sobre a saúde. Ao combinar os dados da saúde com os de outras fontes, o uso pretendido dos dados deve ser claramente definido. Como também se deve respeitar os princípios de GDSAS (exemplo: promover a equidade em saúde e proteger a pessoa) e mitigar os riscos adicionais para a pessoa (exemplo: reidentificação). Isso exigirá uma compreensão flexível de quais dados estão sob a alçada da GDSAS. A GDSAS, portanto, não deve se tornar indevidamente restritiva em relação a novos tipos e novas categorias de dados, pois eles podem oferecer oportunidades relevantes para os sistemas de saúde.

6.3 Construir uma infraestrutura de dados sobre a saúde pública

O desenvolvimento e o fortalecimento da infraestrutura pública digital (incluindo dados) facilitaria a prestação de serviços de saúde e a inovação. Essa infraestrutura reuniria dados em tempo real de muitas fontes e os disponibilizaria de maneira segura e contínua para provedores e inovadores de serviços de saúde. A infraestrutura pública digital poderia servir como um mecanismo proativo e flexível para inovações técnicas e de processo.

6.4 Empregar políticas inovadoras

A política e a legislação podem estar atrasadas em relação às capacidades tecnológicas de coleta, processamento e uso de dados, incluindo o surgimento de novas tecnologias digitais e a criação de novos modelos de negócios. Novas políticas com estruturas mais amplas, cobrindo vários cenários possíveis e emergentes, podem ser necessárias. Instalações de "caixas de areia" e uso informal e temporário de padrões ou práticas emergentes são exemplos de inovação política. Tais inovações devem orientar a utilização de tecnologias emergentes para o uso apropriado de dados sobre a saúde (exemplo: desenvolvimento da medicina de precisão ou aplicação de *Big Data* para desenvolvimento de novos dispositivos médicos). As novas abordagens políticas devem orientar as inovações baseadas

em dados para alcançar a equidade em saúde e garantir a Cobertura Universal de Saúde.

7. Princípio VII – Promover benefícios equitativos dos dados sobre a saúde

A equidade deve ser inerente à GDSAS, ao garantir uma representação equitativa nos dados de todas as pessoas, dos grupos e das comunidades, independentemente de características sociais ou econômicas, bem como assegurar o acesso equitativo ao valor da saúde originado dos dados. A governança equitativa reforça as necessidades de criação de aplicações de dados de saúde que abranjam as diferentes populações nos serviços e sistemas de saúde. Também promove o compartilhamento equitativo de melhorias e inovação dos serviços de saúde orientados por dados, especialmente com a contribuição das pessoas e comunidades, que fornecem esses dados. A equidade na GDSAS deve se estender além de políticas, processos e resultados, e incluir o engajamento público, a educação e a participação significativa de todos, na tomada de decisão acerca dos sistemas de dados sobre a saúde. Discorremos sobre os elementos centrais do princípio VII nos próximos subitens.

7.1 Representar todos os grupos e as populações de forma equitativa nos dados

Os dados sobre a saúde de todos os grupos e das populações devem ser inclusivos e representativos de forma equitativa, independente dos atributos demográficos ou sociais (exemplo: sexo, identidade de gênero, raça, etnia, *status* de cidadania, *status* de refugiado, identidade sexual, capacidade) ou das características econômicas (exemplo: nível educacional, situação de renda, profissão). Isso requer metodologias e processos de coleta de dados inclusivos que considerem: quem são solicitados a fornecer os dados; as categorias de dados; e o uso pretendido.

7.2 Considerar as necessidades específicas de grupos e populações marginalizados

Para considerar de forma equitativa as necessidades específicas de grupos e das populações marginalizadas relacionadas à GDSAS, a coleta e a análise de dados devem ser interseccionais e transversais, ao longo de categorias sociodemográficas e econômicas. A GDSAS também deve atender às necessidades específicas de proteção de grupos e populações marginalizados – como, por exemplo, expor informações sobre identidade sexual e de gênero pode colocar pessoas em risco de

prisão ou de violência, em alguns contextos. Esses grupos devem ser envolvidos, efetivamente, no desenvolvimento, na implementação e na revisão de políticas e de práticas de governança.

7.3 Atenuar o viés dos dados

O viés pode ser introduzido em qualquer ponto da coleta, no processamento, no uso de dados etc. Esse viés pode perpetuar desigualdades, minar a integridade dos dados e levar a interpretações incorretas ou incompletas. O preconceito também leva à discriminação e à exclusão, intencional ou não. A GDSAS deve ter como objetivo identificar onde está o viés e neutralizar os seus efeitos, criar mecanismos para relatar e abordar os preconceitos existentes nos sistemas e proteger os envolvidos e seus dados contra o uso indevido e contínuo.

7.4 Usar linguagem acessível e preencher as lacunas do conhecimento

A GDSAS deve ser compreensível para o público em geral e escrita em linguagem neutra, em termos de gênero, ser acessível às crianças e àqueles com baixo nível de alfabetização e sem tanta familiaridade com idiomas menos populares. Embora documentos jurídicos ou técnicos específicos possam ser necessários para legislar ou operar a GDSAS, os recursos de apoio devem melhorar a compreensão de pessoas e comunidades sobre seus direitos, de maneira prática e acionável. Esforços devem ser feitos para aumentar o conhecimento do público sobre a GDSAS e o seu impacto individual e social.

7.5 Implementar mecanismos inclusivos de retorno sobre os dados utilizados

Devem ser estabelecidos mecanismos de retorno para que pessoas, comunidades e instituições estejam cientes de como os dados são utilizados em cada etapa do ciclo de vida dos dados. Os que fornecem seus dados e os envolvidos na coleta de dados sobre a saúde (exemplo: profissionais de saúde na linha de frente) devem compreender o propósito e os resultados dessa utilização. Pessoas e comunidades também devem ter controle sobre seus dados e ser capazes de tomar decisões apropriadas por si mesmos. Garantir isso apoiará o envolvimento significativo da sociedade civil, durante a fase de coleta de dados e em outras fases.

7.6 Promover impacto e benefício equitativos

A GDSAS deve garantir que o benefício do uso de dados e dos sistemas de saúde orientados por dados seja compartilhado de forma equitativa entre todos

os grupos e populações, independente das características sociais, econômicas ou políticas. Isso pode implicar melhoria do desenho, alcance e acessibilidade desses sistemas para incluir as necessidades de diversos grupos e populações. Os benefícios obtidos devem ser compartilhados de forma justa e equitativa com aqueles que contribuem com dados. Além disso, são necessárias medidas proativas para garantir que o uso e os sistemas visem especificamente à prestação de serviços de saúde equitativos e de alta qualidade para grupos marginalizados.

8. Princípio VIII – Estabelecer direitos de propriedade sobre os dados

A GDSAS deve estar enraizada em direitos relacionados aos dados. Normas, princípios, políticas e leis devem ser extraídas de tais direitos abrangentes. Isso inclui a consideração de todos os direitos humanos, incluindo o direito à proteção e à segurança, e o direito de se beneficiar equitativamente dos dados fornecidos, em níveis individual e comunitário. A propriedade dos dados implica que todos têm o direito de conhecer, determinar e controlar como seus dados são usados. Esses direitos se estendem a produtos e serviços derivados de dados, como a IA. Sistemas de dados sobre a saúde e a sua governança devem ser projetados com base em tais direitos e propriedade de dados. Os elementos centrais do princípio VIII estão tratados a seguir.

8.1 Aplicar a visão dos direitos humanos à GDSAS

Os direitos humanos – conforme expressos em documentos como a "Declaração Universal dos Direitos Humanos", o "Pacto Internacional sobre Direitos Civis e Políticos" e o "Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais" – devem ser centrais à articulação dos direitos e da posse dos dados. Muitos direitos, incluindo os tradicionais (exemplo: segurança, saúde) e os novos associados aos dados (exemplo: privacidade), aplicam-se aos vários cenários de uso de dados (exemplo: os direitos relacionados à segurança das mulheres ou dos trabalhadores podem ser aplicáveis em um determinado contexto ou processo de uso de dados). Os direitos individuais e coletivos de populações marginalizadas devem receber atenção especial.

8.2 Definir papéis e responsabilidades de governança claros

Para garantir os direitos sobre os dados e a sua propriedade, é importante definir claramente vários papéis relevantes relativos aos sistemas de dados sobre a saúde,

incluindo o proprietário, o custodiante, o processador, o administrador de dados e o beneficiário do uso dos dados. Esses papéis devem elucidar quem tem e quem garante que os direitos sejam respeitados. Essas funções devem incluir responsabilidades muito bem definidas, sobretudo as relativas à privacidade, à proteção de dados e ao compartilhamento de benefícios. As definições usadas nas diretrizes de governança de dados existentes (exemplo: GDPR, PDPA, LGPD no Brasil), e outras estruturas emergentes, podem ser adaptadas ou usadas nesse sentido.

8.3 Normatizar os direitos e a propriedade dos dados

Os direitos e a propriedade dos dados devem ser regulados por legislação e na política em alinhamento com normas, leis e regulamentos regionais, nacionais e globais, que sejam atuais e emergentes. Isso deve incluir definições de propriedade dos dados (exemplo: os dados sobre a saúde são de propriedade da pessoa ou da comunidade que os fornece) e de direitos relacionados (exemplo: direito de controlar o uso, de recusar a participação na coleta, de retirar de um sistema, direito ao benefício). Além disso, o direito de acesso pode ser diferente de ter a propriedade desses dados. Essas definições devem estar vinculadas às funções e às responsabilidades definidas pelos interessados nos dados sobre a saúde. A GDSAS deve delinear e fornecer os mecanismos para o exercício desses direitos e da propriedade.

8.4 Estender direitos e propriedade de dados a produtos e serviços

Os direitos e a propriedade de dados vão além dos dados para produtos e serviços relacionados, como IA. Os dados usados não devem prejudicar pessoas ou comunidades e os produtos e serviços derivados também não devem causar danos. Da mesma forma, a propriedade individual e comunitária se estende ao direito de compartilhar os benefícios equitativos dos produtos e serviços derivados do uso.

8.5 Desenvolver fundos de dados sobre a saúde e cooperativas de dados sobre a saúde

Para uma implementação eficaz dos direitos e da propriedade de dados sobre a saúde, bem como um amplo compartilhamento de dados, devem ser desenvolvidos fundos e cooperativas de dados sobre a saúde. Tais instituições definem as regras do ciclo de vida dos dados, respeitando os direitos de dados e a propriedade de pessoas e comunidades, enquanto fornece ativamente meios para exercê-los. São um meio apropriado para compartilhar dados com segurança em um cenário de

saúde mais amplo. Eles podem ser executados por terceiros que sejam neutros ou representantes dos titulares dos dados.

8.6 Empregar mecanismos participativos de governança de dados

Normas, princípios, políticas, regras e práticas de governança de dados devem ser desenvolvidos de forma aberta e participativa. Isso pode incluir mecanismos como grupos de trabalho com membros representativos, livros-brancos[53] e consultas públicas. A participação proativa de grupos marginalizados deve ser assegurada. A GDSAS deve fornecer mecanismos contínuos para a participação significativa de pessoas e comunidades, quando os dados são reutilizados, incluindo meios para reafirmar o consentimento diante das necessidades de novos dados e para receber e abordar as várias dúvidas e preocupações.

8.7 Conectar-se a mecanismos de responsabilização mais amplos

A GDSAS deve ser integrada a mecanismos formais de responsabilização pública que possam existir em um determinado contexto para garantir a adesão às políticas, às leis e aos direitos relacionados à saúde. Ademais, certos tipos de dados sobre a saúde podem ser úteis e disponibilizados para os esforços de monitoramento e responsabilização liderados pela sociedade civil.

Considerações finais

No Brasil, a Associação Brasileira de Saúde Coletiva (Abrasco) tem discutido e disseminado a questão da proteção dos dados em suas propostas – mais especificamente no Plano Diretor para o Desenvolvimento da Informação e Tecnologia de Informação em Saúde (PlaDITIS) (Silva *et al.*, 2020) – o que vem influenciando decisivamente a política nacional sobre o tema (Brasil, 2020).

Em sua terceira edição, o PlaDITIS (Abrasco, 2020) alerta para a falta de governança na condução da informatização das redes de atenção do SUS, em especial a porta de entrada, composta de Unidades Básicas de Saúde (UBS) e Núcleos de Apoio à Saúde da Família (NASF), cuja responsabilidade é municipal e prevista na Constituição brasileira.

Espera-se com a disseminação desses princípios entre pesquisadores do campo da saúde coletiva, profissionais de saúde e professores estimular o debate multidisciplinar no país sobre a condução ética da digitalização dos

53 Proposta ou rascunho de documento oficial elaborado por um governo ou uma organização a fim de servir como guia ou informe sobre ações específicas a serem tomadas.

registros de saúde dos cidadãos e a garantia de seus direitos. Os dados digitalizados são extensões das pessoas naturais, trazem benefícios para o campo da saúde, como o uso da telessaúde para atender aos povos isolados. No entanto, o uso indevido dessa informação em rede traz novos desafios. Trata-se de um problema a ser ponderado e regulado, globalmente, contemplando a multiplicidade humana.

Referências

ABRASCO. ASSOCIAÇÃO BRASILEIRA DE SAÚDE COLETIVA. **3º Plano diretor para o desenvolvimento da informação e tecnologia de informação em saúde**. 3º PlaDITIS: 2020-2024. Rio de Janeiro: Associação Brasileira de Saúde Coletiva, 2020. Disponível em: file:///C:/Users/maria/Desktop/Plano%20Informa%C3%A7%C3%A3o%20e%20TI%20em%20saude%20ABRASCO.pdf. Acesso em: 7 fev. 2024.

BRASIL. Presidência da República. **Decreto n. 591, de 6 de julho de 1992**. Atos Internacionais. Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais. Promulgação. 1992a. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0591.htm. Acesso em: 2 fev. 2024.

BRASIL. Presidência da República. **Decreto n. 592, de 6 de julho de 1992**. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. 1992b. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 2 fev. 2024.

BRASIL. Presidência da República. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 15 jan. 2024.

BRASIL. Presidência da República. **Lei n. 8.080, de 19 de setembro de 1990**. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, e o funcionamento [...]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8080.htm#:~:text=LEI%20N%C2%BA%208.080%2C%20DE%2019%20DE%20SETEMBRO%20DE%201990.&text=Disp%C3%B5e%20sobre%20as%20condi%C3%A7%C3%B5es%20para,correspondentes%20e%20d%C3%A1%20outras%20provid%C3%AAncias. Acesso em: 15 jan. 2024.

GDPR. GENERAL DATA PROTECTION REGULATION. *s.d.* Disponível em: https://gdpr-info.eu/. Acesso em: 12 abr. 2022.

GS1. Global Forum 2024. Disponível em: https://www.gs1.org/. Acesso em: 12 abr. 2022.

HEALTH LEVEL 7. **FHIR v 4.0.1**. *s.d.* Disponível em: http://hl7.org/fhir/. Acesso em: 12 abr. 2022.

ISO. **ISO/TS 22220:2011 Health informatics**. Identification of subjects of health care. 2011. Disponível em: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/05/97/59755.html. Acesso em: 12 abr. 2022.

KICKBUSCH, Ilona *et al. The Lancet* and *Financial Times* Commission on governing health futures 2030: growing up in a digital world. **The Lancet**, v. 398, n. 10312, p. 1727-1776, 6 nov. 2021. DOI: 10.1016/S0140-6736(21)01824-9. Disponível em: https://pubmed.ncbi.nlm.nih.gov/34706260/. Acesso em: 3 jan. 2024.

NKRUMAH, Kwame. Neocolonialismo: último estágio do Imperialismo. Rio de Janeiro: Civilização Brasileira, 1965.

NEW ZELAND GOVERNMENT. **Data Futures Partnership**. *s.d.* Disponível em: https://www.stats.govt.nz/assets/Uploads/Retirement-of-archive-website-project-files/Corporate/Cabinet-paper-A-New-Zealand-Data-Futures-Partnership/nzdf-partnership-overview.pdf. Acesso em: 12 abr. 2022.

OECD/LEGAL/0433. **Recommendation of the Council on Health Data Governance**. 2023. Disponível em: https://legalinstruments.oecd.org/api/print?ids=348&lang=en. Acesso em: 12 abr. 2022.

OECD/LEGAL/0449. **Recommendation of the Council on Artificial Intelligence**. 2019. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Acesso em: 12 abr. 2022.

ONU. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. Disponível em: https://www.ohchr.org/en/human-rights/universal-declaration/translations/portuguese?LangID=por. Acesso em: 29 jul. 2024.

OPAS. ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE. **Oito princípios orientadores da transformação digital do setor da saúde**: um apelo à ação pan-americana. Washington, 2021. Disponível em: https://iris.paho.org/bitstream/handle/10665.2/54669/OPASEIHIS210004_por.pdf?sequence=1&isAllowed=y. Acesso em: 12 abr. 2022.

OPENHIE. *s.d.* Disponível em: https://ohie.org/. Acesso em: 12 abr. 2022.

PDPC | PDPA Overview. *s.d.* Disponível em: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act. Acesso em: 12 abr. 2022.
POPI ACT. PROTECTION OF PERSONAL INFORMATION ACT (POPI Act). *s.d.* Disponível em: https://popia.co.za/. Acesso em: 12 abr. 2022.

SILVA, Angélica Baptista *et al.* Three decades of telemedicine in Brazil: Mapping the regulatory framework from 1990 to 2018. **PLOS ONE**, v. 15, n. 11, p. e0242869, 25 nov. 2020. DOI: https://doi.org/10.1371/journal.pone.0242869. Disponível: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0242869. Acesso em: 5 jan. 2022.

SOUZA, Vanessa de. L. e. **O processo decisório em saúde no Brasil**: gestores, informação e o cuidado à saúde. Tese de Doutorado. Instituto de Comunicação e Informação Científica e Tecnológica em Saúde, Programa de Pós-graduação em Informação e Comunicação em Saúde. Rio de Janeiro, 2018. 280 f. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.arca.fiocruz.br/bitstream/handle/icict/31712/vanessa_souza_icict_dout_2018.pdf?sequence=2&isAllowed=y. Acesso em: 5 jan. 2024.

THE DIGITAL IMPACT ALLIANCE. **Principles for Digital Development**. [Princípios para o desenvolvimento digital]. 2017. Disponível em: https://digitalprinciples.org/. Acesso em: 5 jan. 2024

THE DIGITAL IMPACT ALLIANCE. **The Digital Investment Principles** [Princípios de investimento digital]. 2018. Disponível em: https://digitalinvestmentprinciples.org/. Acesso em: 5 jan. 2024

UNICEF. FUNDO DAS NAÇÕES UNIDAS PARA A INFÂNCIA. **The Case for Better Governance of Children's Data**: A Manifesto. 2021. Disponível em: https://www.unicef.org/globalinsight/media/1741/file/UNICEF%20Global%20Insight%20Data%20Governance%20Manifesto.pdf. Acesso em: 12 abr. 2022.

WHO. WORLD HEALTH ORGANIZATION. **Ethics and governance of artificial intelligence for health**: WHO guidance. [Ética e governança da Inteligência Artificial (IA) para a saúde: orientação da OMS]. Geneva: World Health Organization, 2021. Disponível em: https://www.who.int/publications/i/item/9789240029200. Acesso em: 5 fev. 2024.

WHO. WORLD HEALTH ORGANIZATION. **WHO data principles**. [Princípios de dados da OMS]. 2020. Disponível em: https://www.who.int/data/principles. Acesso em: 12 abr. 2022.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**. Rio de Janeiro: Intrínseca, 2021.

https://doi.org/10.29397/EdicoesLivres/20250110

Assimetrias informacionais e necessidades urgentes: reflexões sobre a cultura de proteção de dados pessoais a partir da experiência da saúde digital no Brasil

Mariana Martins
Natália Fazzioni
Olívia Bandeira

O Brasil aprovou, em agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), passando a fazer parte do conjunto de países que possui uma lei para a proteção da privacidade e o controle dos dados pessoais de seus cidadãos e de suas cidadãs, a exemplo do Regulamento Geral sobre a Proteção de Dados (GDPR, na sigla em inglês), aprovado em 2016 na União Europeia. A legislação brasileira sobre o tema, da mesma forma que o Marco Civil da Internet (lei 12.965/2014), norma legal de referência internacional sobre o uso da internet, foi resultado de um processo que contou com a participação dos diversos setores interessados, além da pressão da sociedade civil para a garantia de direitos no ambiente digital (Coalizão Direitos na Rede, 2018). A LGPD, diferentemente do Marco Civil, estende a proteção de dados pessoais para todos os casos em que eles são utilizados e não somente na internet, regulando a coleta, o uso e o tratamento de dados pessoais feitos em diversas áreas (saúde, educação, comércio, trabalho etc.) e em diferentes tipos de estabelecimentos e tecnologias, como, no caso da saúde, hospitais, postos de saúde, farmácias, aplicativos para celular, aparelhos eletrônicos de controle de índices de saúde, entre outros.

Passados seis anos da aprovação da lei e quatro anos do início da sua vigência, que foi em setembro de 2020, pesquisadores(as), juristas e organizações da sociedade civil consideram que ainda falta um longo caminho para que os direitos regulados na LGPD – e inseridos como direito fundamental na Constituição Federal pela Emenda Constitucional n. 115, de 2022 – sejam efetivados.

Os indícios da necessidade de fortalecimento da lei na prática vão desde os episódios de vazamentos de dados pessoais de grandes proporções que aconteceram no país (Westrup, 2022) até as ações mais cotidianas, em que se observa uma naturalização do fornecimento de dados pessoais a um conjunto crescente de empresas e serviços. Já os motivos elencados para a fragilidade da proteção, apesar dos avanços trazidos pela LGPD, incluem a falta de independência e a estrutura da Autoridade Nacional de Proteção de Dados (ANPD), responsável por regular a LGPD e fiscalizar o seu cumprimento (Westrup, 2022). Além disso, destaca-se o que vem sendo chamado de "ausência de uma cultura de proteção de dados" no país, tema que nos interessa neste capítulo. Como sugeriram Laura Schertel Mendes e Danilo Doneda, em artigo publicado em 2018, além de uma autoridade nacional forte e independente:

> Outro importante desafio diz respeito à mudança cultural, necessária para a eficaz implementação da lei. Afinal, a LGPD traz os princípios da necessidade e da finalidade, que indicam que os dados pessoais somente poderão ser tratados quando o tratamento for necessário para atender às necessidades do controlador de dados e se a sua utilização ocorrer no âmbito do contexto ou de forma compatível com as finalidades para as quais os dados foram coletados. Isto é, faz-se necessária uma verdadeira mudança cultural para incorporarmos a compreensão de que todo dado pessoal é merecedor de proteção jurídica, por ser um meio de representação da pessoa na sociedade. (Mendes; Doneda, 2018, p. 479)

De acordo com Luca Belli e Danilo Doneda (2021), com base em Stefano Rodotà (2008), a cultura de proteção de dados é entendida como "a consciência pelo tecido social da profunda ligação da proteção de dados com as garantias de liberdade, igualdade e democracia" (Belli e Doneda, 2021, s/p). Nessa perspectiva, a proteção de dados está relacionada a uma espécie de mudança de mentalidade em que o direito estabelecido em lei é percebido pelos agentes e garantido a partir de suas ações. Embora esses agentes não estejam nomeados, podemos incluir todos aqueles que fazem parte do que está sendo chamado de "mercado de dados pessoais" (Silveira; Avelino; Souza, 2016): as empresas públicas e privadas, as tecnologias, os produtos e serviços que coletam, tratam e monetizam os dados pessoais, além dos usuários que fornecem seus dados pessoais em suas ações cotidianas.

No entanto, como operacionalizar tal processo de "tomada de consciência" e, acima de tudo, construir possibilidades de ação, em contextos nos quais as próprias

noções de liberdade, igualdade e democracia, citadas acima, são tão frágeis? O que significa falar em "mudança cultural" na proteção de dados pessoais, quando os direitos que a fundamentam – como os de privacidade, de intimidade, de honra e imagem, de liberdade de expressão, de informação, de opinião e de comunicação – estão ainda longe de ser efetivados (Intervozes, 2023)?

Essas são algumas provocações que esse texto sugere, a partir das análises preliminares de alguns dos dados da pesquisa "Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil".[54] A pesquisa tem como pressuposto a importância do reconhecimento do direito à proteção de dados pessoais como algo fundamental diante de uma sociedade cada vez mais permeada pela plataformização (Zuboff, 2021; Van Djick; Poell, 2016) das esferas da vida e pela geração de um significativo mercado de dados pessoais. Para além desse pressuposto, entende-se que houve um significativo aumento dos serviços de saúde digital, nos últimos anos, com maior destaque para o período da pandemia da covid-19, que não só intensificou, mas também acelerou o processo de migração do campo da saúde para o mundo digital. Essa nova realidade fez com que os dados de saúde – considerados sensíveis e, portanto, merecedores de cuidados adicionais pela LGPD – passassem a trafegar em uma velocidade maior do que a fiscalização prevista pela lei pudesse aferir, como também impusessem dificuldades para que os(as) próprios(as) usuários(as), detentores dos dados pessoais, pudessem acompanhar.

A pesquisa considerou os(as) usuários(as)[55] dos serviços de saúde como os principais agentes a partir dos quais investigar a coleta e o uso dos dados pessoais na saúde, por dois motivos principais. Em primeiro lugar, porque os(as) usuários(as) são os sujeitos de direito dos dados pessoais. Em segundo lugar, porque a revisão bibliográfica mostrou que as percepções dos(as) usuários(as) são pouco consideradas nas análises sobre o tema.[56] A pesquisa optou metodologicamente por partir do(a) usuário(a) (no caso, usuários(as) identificados como pacientes de doença crônica) e de seu itinerário de tratamento para pensar os lugares (estabelecimentos de saúde) nos quais os dados pessoais e os dados pessoais sensíveis são fornecidos.

Dessa forma, esse artigo problematiza a ideia de "cultura de proteção de dados pessoais", a partir das percepções dos(as) usuários(as) traçadas por meio de 16

54 Pesquisa realizada pelo Instituto de Comunicação e Informação Científica e Tecnológica em Saúde (Icict) da Fiocruz, em parceria com o Intervozes – Coletivo Brasil de Comunicação Social e o Instituto Brasileiro de Defesa do Consumidor (Idec). Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.icict.fiocruz.br/sites/www.icict.fiocruz.br/files/resumo_executivo_protecao_de_dados_pessoais.pdf. Acesso em: 20 jan. 2024.

55 Utilizamos o termo usuário que é corrente tanto no sistema de saúde como nos debates sobre uso da internet.

56 A revisão bibliográfica coletou 105 trabalhos dentro do escopo e analisou 82 deles, de acordo com os critérios de exclusão estabelecidos.

entrevistas em profundidade, realizadas com usuárias/usuários dos serviços de saúde que vivem com diabetes. As entrevistas tinham o objetivo de trazer, entre outras questões, a percepção desses agentes sobre a proteção de dados pessoais, os riscos, as vulnerabilidades e as ações de mitigação desses riscos. Além disso, consideramos que o tema ganha complexidade, quando assumimos as profundas desigualdades socioeconômicas que caracterizam a sociedade brasileira e também o lugar do Brasil, como um país considerado periférico, no mercado mundial de dados pessoais.

Trabalhar com o conceito de "cultura" é sempre um desafio nas ciências sociais e humanas. Esse é um tema caro à sociologia, à antropologia e aos estudos comunicacionais. Mesmo que estejamos aqui qualificando e especificando esse termo como cultura de proteção de dados pessoais, conforme vem sendo tratado na bibliografia, e ainda mais precisamente como cultura de proteção de dados pessoais no contexto da saúde, precisamos expressar nosso cuidado ao utilizar um conceito já amplamente estudado e problematizado na literatura (Williams, 1979; 2011; Thompson, 1995; Appadurai, 1995; Clifford, 1988; Abu-Lughod; Rego; Durazzo, 2018). Em um dos seus mergulhos sobre este conceito, Williams alerta para a complexidade do tema:

> A complexibilidade do conceito de "cultura" é, portanto, notável. Tornou-se um nome do processo "íntimo", especializado em suas supostas agências de "vida intelectual" e "nas artes". Tornou-se também um nome de processo geral, especializado em suas supostas configurações de "modos de vida totais". Teve um papel crucial em definições de "artes" e "humanidades", a partir do primeiro sentido. Desempenhou papel igualmente importante nas definições das "Ciências Humanas" e "Ciências Sociais", no segundo sentido. Cada tendência se inclina a negar o uso do conceito à outra, apesar de muitas tentativas de reconciliação. (Williams, 1979, p. 24)

Sem pretensão de esgotar a discussão sobre os conceitos possíveis de cultura, e mesmo as críticas ao conceito e ao que ele produz, ilustramos apenas a complexidade do tema e compartilhamos da premissa antropológica de que cultura não pode ser entendida de forma universal e singular, sendo, portanto, necessário apontar para a pluralidade e complexidade de fenômenos globais vistos a partir de contextos específicos – desafio que vem sendo enfrentado de forma cada vez mais complexa desde que a globalização avançou, a partir

do desenvolvimento das tecnologias e das novas formas de conectividade (Appadurai, 1995; Hannerz, 1997). Desafio esse, ainda mais complexo, quando determinantemente marcado pelo que tem sido chamado mais recentemente de colonialidade do poder (Quijano, 2005).

Propomos, assim, entender a noção de cultura de proteção de dados pessoais, enquanto algo que não está dado, ou seja, não está posto como uma cartilha de práticas a serem seguidas, importada de contextos outros (sobretudo europeus), mas como uma síntese entre fluxos globais do mercado de dados pessoais e particularidades da realidade brasileira e dos diferentes grupos sociais que a compõem em constante processo de produção e transformação. Ou seja, mais do que algo que se "possui" ou não, a cultura de proteção de dados pessoais é algo que se deve construir localmente, diante de um fenômeno marcado pelo mercado de dados, cuja consolidação na América Latina é extremamente particular. Construir localmente políticas que afetem o fluxo de poder global é, contudo, um dos grandes desafios dos chamados países periféricos submetidos à colonialidade e ao modelo neoliberal.

Resgatando as discussões feitas por Quijano, Couldry e Mejias sobre colonialidade e colonialismo de dados, Sérgio Amadeu da Silveira (2021) pontua a realidade dos países periféricos e a materialidade desse pensamento por meio da perpetuação de mentalidades, de relações de subordinação, sujeição e inferiorização, de modos de vida, saberes e conhecimentos que ilustram a dificuldade de construção, entre outras coisas, de padrões próprios ou locais.

> As corporações sempre estão prontas a nos servir, serão mais rápidas do que construir um caminho de aprendizado e de fortalecimento das inteligências locais. No contexto da colonialidade, o colonizado, a inteligência coletiva local, nunca está pronto, apto, capacitado para enfrentar um problema sem recorrer a uma corporação da matriz. O neoliberalismo se aconchega na colonialidade. (Silveira, 2021, p. 41)

A partir dessa perspectiva, fundamentamos nosso olhar para os discursos dos(as) usuários(as) aqui apresentados. Interessa-nos observar de que forma esses(as) usuários(as) entendem a proteção de dados pessoais e de que forma as percepções sobre o assunto são acionadas nas vivências cotidianas deles, considerando, no caso estudado, as especificidades do uso de dados pessoais na saúde, em particular para usuários(as) com doenças crônicas, que utilizam de forma intensa os serviços e as tecnologias de saúde.

1. A proteção de dados pessoais e o direito à comunicação

O conceito de proteção de dados pessoais deriva, mas não se confunde, com o direito à privacidade. Ele emerge em um contexto relativamente novo em que, devido à digitalização de inúmeros aspectos da vida, o cidadão e a cidadã perdem facilmente o controle sobre os seus dados pessoais. Dado pessoal, segundo Mendes (*apud* Silva *et al.*, 2020, p. 580), é todo dado relacionado a uma pessoa singular que possa ser identificada, direta ou indiretamente, por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica, um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular. E, dessa forma, o direito à proteção de dados pessoais:

> [...] é reconhecido como uma espécie do direito fundamental à privacidade (Peixoto; Ehrhardt Junior, 2018) e alicerça-se na autodeterminação informativa, isto é, sinteticamente, no direito de cada indivíduo decidir quando e como dispor de suas informações. (Silva *et al.*, 2020, p. 580).

Danilo Doneda (2011) defende que a proteção de dados pessoais está diretamente ligada à proteção dos direitos humanos e das liberdades fundamentais, entendendo-a como pressuposto do Estado democrático, tendo como marco a Convenção de Strasbourg.

A legislação distingue também a existência de dados pessoais sensíveis, ou seja, dados que, por seu potencial de interferir na privacidade e nos demais direitos dos sujeitos, demandam um cuidado maior e, portanto, um regime jurídico diferenciado. Segundo a LGPD, são dados pessoais sensíveis aqueles que tratam:

> [...] 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, 2018)

Embora a LGPD (art. 46 § 1º) preveja que é de responsabilidade dos agentes de tratamento de dados tomar medidas técnicas e organizacionais para prever, proteger e averiguar a ocorrência de incidentes de segurança envolvendo dados pessoais, cabe ao(à) usuário(a) o direito ao acesso à informação e o consentimento

ou não sobre o uso dos seus dados. Como promover, então, uma cultura de proteção de dados pessoais entre usuários(as) brasileiros(as)?

Como já afirmado anteriormente, faz-se necessário considerar a desigualdade estrutural da sociedade brasileira em diferentes aspectos e também as desigualdades e fragilidades dos(as) usuários(as) no mercado de dados pessoais – o que acarreta em uma enorme "assimetria" informacional diante dessa temática. De acordo com Linke (2019, p. 181-182):

> [...] o consumidor, além da vulnerabilidade que lhe é inerente, encontra-se em uma situação cuja assimetria informacional é abissal, sequer possui conhecimento dos possíveis usos de seus dados, quem terá acesso, por quanto tempo, e as possíveis futuras repercussões negativas em sua vida.

Apesar disso, interessa-nos ver, nas entrevistas realizadas nessa pesquisa, quais percepções os(as) usuários(as) têm sobre essas questões. Esses agentes e as suas opiniões nos interessam para aprofundar as relações entre direito à comunicação e direito à saúde.

As entrevistas com os(as) usuários(as) mostram que, por um lado, há falta de informação sobre o que é possível ser feito com os dados pessoais e com as informações geradas (dados tratados), a partir de bases de dados. Isso faz com que a preocupação sobre os possíveis riscos, como os relativos à modulação de comportamentos e às situações de discriminação, pouco apareça (Silveira; Avelino; Souza, 2016). Por outro lado, mesmo quando o(a) cidadão(ã) tem uma percepção dos possíveis riscos, nem sempre ele(ela) tem condições de abrir mão do que se oferece em troca dos dados pessoais, considerando, como veremos, que a situação é inevitável. Ou seja, diante do mercado de dados pessoais, a privacidade como um direito é um debate que está longe de ser consolidado.

2. A proteção de dados pessoais na visão de pessoas com diabetes

Para que se entenda um pouco melhor os recortes utilizados neste trabalho, cabe lembrar que os resultados analisados aqui fazem parte de uma pesquisa maior que tem como objeto a análise da proteção de dados pessoais em serviços de saúde digital e, portanto, foram feitas algumas escolhas metodológicas. Como, por exemplo, a delimitação de um território inicial, no caso o Recife, e a seleção de um grupo específico de usuários(as), no caso, pessoas com doenças crônicas e, mais especificamente, diabetes. A decisão de delimitar os(as) usuários(as), a partir de

uma enfermidade crônica, baseou-se no alto fluxo de uso dos serviços de saúde desses pacientes. No caso da diabetes, sobretudo, considerou-se a prevalência dessa doença na população brasileira e a importância do desenvolvimento tecnológico no manejo da doença (voltado para uso de medidores de glicose, sistemas de contagem de carboidratos, bombas de insulina, entre outros).

Esses grupos de usuários(as) têm seus dados pessoais sensíveis sistematicamente coletados, seja pelo sistema de saúde, seja por provedores de serviço/aplicações em saúde digital e por empresas prestadoras de serviços de saúde, como planos de saúde, laboratórios farmacêuticos e farmácias. A pesquisa buscou, portanto, saber que tipos de dados são comumente fornecidos por esses grupos de usuários(as), por meio de quais dispositivos e plataformas digitais, e a percepção que eles têm sobre a coleta e o uso de dados pessoais sensíveis.

Foram realizadas 16 entrevistas em profundidade com usuários(as) dos sistemas público e privado de saúde. Cabe ainda destacar que a pesquisa chegou aos(às) usuários(as) entrevistados(as) majoritariamente por meio da interlocução estabelecida com a Associação de Diabetes Juvenil[57] (ADJ), cuja parceria foi de extrema importância –, o que nos levou também a ampliar o território para além do Recife.

Partindo desse diálogo, foram definidos três tipos de usuários(as) que poderiam contribuir com a temática da pesquisa: usuários(as) influenciadores digitais; usuários(as) que atuam profissionalmente na associação; e usuários(as) associados(as) à ADJ sem atuação específica, sendo esses três grupos compostos por pessoas com diabetes.[58] Dessa forma, a maior parte dos entrevistados (10 pessoas) concentrou-se no estado de São Paulo, onde se localiza a ADJ e uma parte considerável de seus associados. O segundo grupo (5 pessoas) está localizado no estado de Pernambuco. E, finalmente, entrevistamos uma pessoa no Rio de Janeiro. O grupo total é constituído por 56,3% de mulheres e 43,7% de homens. Com relação à faixa etária, há uma significativa heterogeneidade que

57 A ADJ é uma das entidades que compõem o Conselho Nacional de Saúde (CNS). Como uma das representantes da sociedade civil, foi fundamental para nos ajudar a encontrar entrevistados e passar a eles a confiança necessária para a realização das entrevistas. Inicialmente, a ADJ se concentrou em indicar para as entrevistas usuários(as) da cidade do Recife, território definido para a realização do trabalho de campo. Entretanto, ao constatar a dificuldade em localizar os associados nessa cidade, ampliou-se o escopo para outras cidades, entendendo que as experiências com a saúde digital extrapolavam o espaço dos serviços de saúde tradicionais e que, portanto, não comprometeria nem representaria prejuízo ao resultado final da pesquisa.

58 No primeiro grupo, usuários(as) influenciadores digitais – procurou-se entender de que formas as tecnologias e a proteção de dados se inserem na produção não especializada de difusão de informações em saúde voltada para pacientes com doenças crônicas. Também buscou-se saber de que formas tais atores sociais se articulam com gestores públicos e empresas de desenvolvimento de tecnologias em saúde. Nesse grupo, foram entrevistadas três influenciadoras, uma de São Paulo, uma do Recife e outra do Rio de Janeiro. No segundo grupo, usuários(as) da sociedade civil organizada – foi realizado um grupo focal com quatro representantes da ADJ, todos com base na cidade de São Paulo. Eles também se inserem na categoria de usuários(as) do sistema de saúde. Além de terem informações sobre as experiências dos usuários(as) nos sistemas de saúde, as associações também são agentes que coletam e tratam dados de usuários(as). No último grupo, usuários(as) associados(as) à ADJ sem atuação específica – foram entrevistados nove usuários(as) indicados(as) pela ADJ, com variedade de gênero, raça, idade e origem socioeconômica. Nos três grupos procurou-se compreender seus itinerários por serviços de saúde e sua percepção sobre tecnologia na área da saúde e sobre proteção de dados pessoais.

inclui pessoas de 18 até 90 anos, com distribuição similar entre as diferentes faixas.

Ao contar sobre seus cuidados com a saúde, os(as) usuários(as) foram provocados pelos entrevistadores a refletir sobre o fornecimento de seus dados pessoais: onde e em que circunstâncias costumam fornecer seus dados pessoais? Que dados fornecem? Para que finalidade os dados são coletados? Quem armazena esses dados?

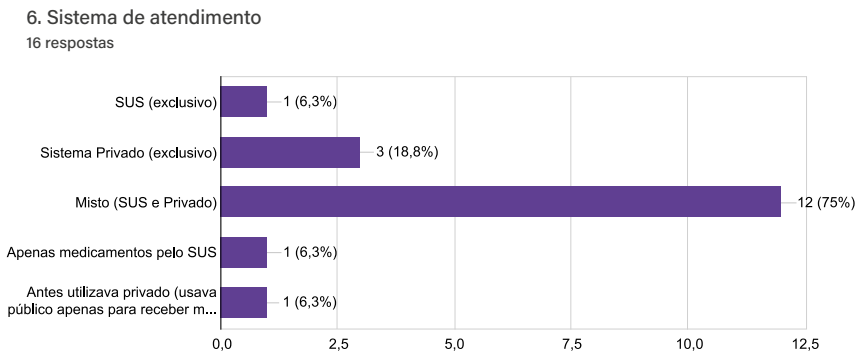
A partir das entrevistas, pudemos identificar discursos que nos ajudam a pensar e a contribuir com as reflexões em torno da discussão da cultura de proteção de dados pessoais no Brasil, principalmente perceber os desafios que esse conceito nos traz. O quão a LGPD consegue ser apropriada pelos(as) usuários(as)? O que significa na vida prática a proteção de dados pessoais ter se tornado um direito fundamental no Brasil? Como isso se reflete no discurso dos(as) usuários(as) dos serviços de saúde digital, que para além de dados comuns, costumam compartilhar dados sensíveis? Essas foram algumas das inquietações que surgiram na análise das entrevistas e que serão aqui brevemente discutidas, a partir da apresentação dos Itinerários de saúde dos(as) usuários(as) (item 2.1).

Após apresentar os dados gerais desses itinerários, abordaremos a ideia de cultura de proteção de dados pessoais, a partir das percepções dos(as) usuários(as) dos serviços de saúde digital sobre proteção de dados pessoais e os riscos e as vulnerabilidades associados à coleta e ao tratamento de seus dados pessoais.

2.1 Itinerários de saúde dos(as) usuários(as): das necessidades urgentes aos programas de desconto

Os postos de saúde, os ambulatórios ou consultórios de especialistas, as clínicas de exame (os laboratórios) e as farmácias foram os espaços mais citados pelos(as) usuários(as) com relação ao trânsito para efetivar os cuidados necessários com a saúde e por onde deixam também uma série de dados pessoais. Uma primeira constatação que chamou a atenção com relação aos itinerários dos(as) usuários(as) é que 75% deles utilizavam, simultaneamente, o sistema público e o privado, transitando de formas diferentes entre eles, como podemos verificar no gráfico a seguir (1).

Gráfico 1 - Itinerários - Sistema(s) de atendimento



Uma das usuárias narrou sobre o fluxo desse itinerário entre sistemas:

> Eu, hoje em dia, faço uso tanto do sistema público como do privado. A minha endocrinologista é do SUS, do hospital em que minha mãe trabalha, e quanto aos exames e a todo o resto eu sou acompanhada pelo plano de saúde. Eu sou usuária da bomba de insulina e recebo todos os meus insumos pela rede pública, pelo SUS. (Usuária influenciadora digital, 29 anos, Recife – PE)

No caso dos diabéticos, a retirada de insulina e insumos parece ser o principal fator que vincula os(as) usuários(as) que têm plano de saúde ao sistema público. Por outro lado, a ausência de tecnologias mais sofisticadas e atualizadas de cuidado com a diabetes configura-se como o elemento que mais afasta os(as) usuários(as) do sistema público e os(as) impulsiona a procurar o sistema privado. Isso pode ocorrer tanto em busca dos dispositivos portáteis (medidores de glicose, bombas) como em razão da própria insulina, que pode faltar ou não ser do tipo mais adequado para o paciente, como se observa nas declarações seguintes:

> No começo do tratamento, o tipo de insulina que usava, eu conseguia pela Farmácia Popular. Quando mudei de insulina, a partir daí, eu passei a comprar. (Usuária influenciadora digital, 35 anos, Rio de Janeiro – RJ)

> Consigo pegar as insulinas. Faço uso de dois tipos de insulina, a lenta e a outra, a rápida, consigo pegar as fitas e as agulhas. Porém, em alguns meses faltam algumas coisas. Já passei, por exemplo, oito meses sem receber a insulina ultrarrápida. Já

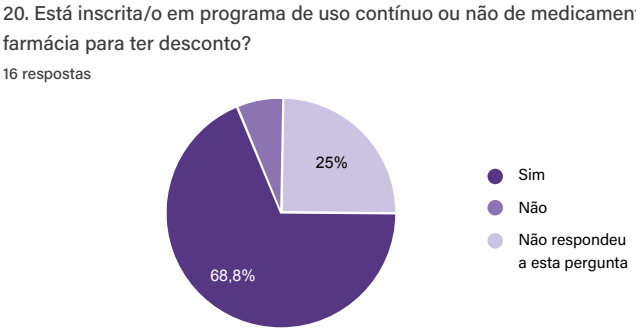
> passei, também, três meses sem receber a insulina lenta. Nesses períodos que faltam, o paciente tem que comprar. Mês passado, por exemplo, também não vieram fitas e tive que comprar. (Usuário sem atuação específica, 22 anos, Serra Talhada – PE)

O acesso às tecnologias para o cuidado com a saúde é narrado pelos(as) usuários(as) como um benefício para a qualidade de vida. Ao mesmo tempo, também são narradas as dificuldades para o acesso. É, assim, que em alguns casos chegam mesmo a judicializar as demandas de saúde para obtenção de dispositivos e insumos tecnológicos para o tratamento da diabetes. Como observa a entrevistada a seguir, ao falar de seu processo de aquisição da bomba de insulina, vemos que só foi possível, a partir da judicialização do convênio:

> Passei um mês com a bomba de insulina sem o sensor, na época. Após um mês, gostei e me adaptei e achei que seria melhor para o meu tratamento. Passei mais um tempo, fiz o pedido pelo plano de saúde, que foi negado. É negado para todos, e entrei com uma ação judicial para conseguir a bomba. Mas só pedi ano passado, acho que em julho ou agosto. Recebi em dezembro de 2020 e comecei a usar em janeiro de 2021. Estou há sete meses mais ou menos fazendo uso. (Usuária influenciadora digital, 29 anos, Recife – PE).

> O acesso aos dispositivos e aos insumos para o tratamento da diabetes é também o que normalmente mobiliza uma frequência intensa das pessoas com diabetes às farmácias e à inscrição em programas de desconto dos laboratórios ou das próprias farmácias para compra de insumos e medicamentos. Durante as entrevistas, esses espaços se revelaram centrais na circulação dos(as) usuários(as) que fornecem dados para descontos de medicamentos de uso contínuo que articulam laboratórios e redes de farmácia. Conforme demonstra o gráfico a seguir (2), 68,8% dos entrevistados afirmaram estar cadastrados em algum desses programas.

Gráfico 2 - Itinerários - Inscrição em programas de descontos



Nas tabelas a seguir (1 e 2), encontram-se as redes de farmácias e os laboratórios citados e o número de vezes em que foram mencionados no conjunto total de entrevistas:

Tabela 1 - Redes de farmácias citadas

Redes de farmácia	**Número de ocorrências**
Drogasil[59]	6
Drogaria São Paulo	5
Droga Raia	5
Rede Farma Popular	1

Tabela 2 - Laboratórios citados

Laboratórios	**Número de ocorrências**
Novo Nordisk	2
Sanofi	2
Johnson	1

59 As redes Drogasil e Droga Raia compõem uma única rede com nomes distintos nas diferentes regiões do país. O grupo RD (Raia Drogasil Gente, Saúde e Bem-Estar S.A.) pertence a Antônio Carlos Pipponzi e é, segundo informações, a empresa líder no mercado brasileiro de varejo farmacêutico, presente em todos os estados brasileiros, com 2,5 mil farmácias tendo registrado um faturamento de R$25,6 bilhões em 2021. O grupo tem outras marcas ligadas à saúde e ao cuidado. Para além disso, o grupo administra uma plataforma de fidelidade, o Stix, que acumula e troca pontos por recompensas. O Stix é "uma plataforma de prêmios das grandes marcas do seu dia a dia". Dessa forma, a plataforma conta ainda com o compartilhamento de pontos com marcas como Pão de Açúcar, Extra, Bike Itaú, Slow Beauty, Desviantes e Instaviagem. Disponível em: https://ri.rd.com.br/show.aspx?idCanal=6aULUwMyMFpYyWDTxjQNnQ==. Acesso em: 11 jul. 2022. Disponível em: https://www.soustix.com.br/sobre-a-stix. Acesso em: 11 jul. 2022.

Sobre o processo que levou ao cadastramento nos programas de laboratórios, uma usuária que é mãe de um adolescente com diabetes, revela:

> As insulinas que ele usa terminam forçando a barra para os cadastrados. Um cadastro que dá um desconto significativo. Por se tratar da medicação de uso contínuo e ser considerada aos análogos de insulina de melhor, digamos assim, de melhor resposta. Então, nós nos cadastramos no programa [...]. (Mãe de usuário adolescente sem atuação específica, 45 anos, Recife – PE)

Como atenta a mesma usuária, esse mesmo tipo de cadastro também possibilita outras formas de atendimento em saúde. Ela prossegue:

> Esse programa dá ao paciente direito ao atendimento *on-line*, se ele quiser, nutricionista, apoio psicológico, certo, é como se fosse um SAC. Se há alguma dificuldade no manejo das canetas também está dentro do programa. Além do desconto na caneta, o uso do insumo, as agulhas [...]. (Mãe de usuário adolescente sem atuação específica, 45 anos, Recife – PE)

Para os(as) usuários(as), outra vantagem oferecida por esse tipo de cadastro, além do desconto e dos serviços, é a integração a uma rede de descontos em diferentes setores, que inclui lojas de departamento, supermercados e planos de saúde (convênio). Como revela uma das entrevistadas:

> Meu cartão Riachuelo, que é da loja Riachuelo, ele dá desconto na farmácia também [...]. Só que aí como eu tenho convênio, no convênio tem desconto, eles verificam qual tem maior desconto. (Usuária sem atuação específica, 25 anos, Osasco – SP)

Outras empresas citadas nesse mesmo sentido foram: Lojas Marisa, Supermercado Dia, Supermercado Pão de Açúcar e Posto Ipiranga – Aplicativo "Abastece aí".

É interessante observar que os itinerários de saúde dos pacientes com diabetes são profundamente afetados por padrões de consumo e possibilidade de acesso ao desenvolvimento tecnológico na área, com impactos positivos e negativos das diferentes e complexas formas de itinerários de saúde aqui apresentadas. Assim, fica evidente que tais itinerários consolidam-se para além das relações com especialistas e serviços de saúde *stricto sensu*, passando por uma série de

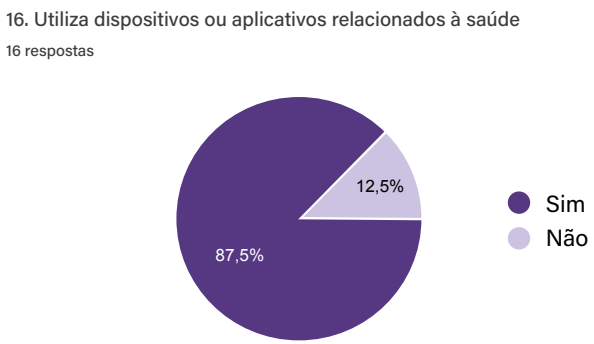
outras esferas, inclusive, a do fornecimento de dados pessoais em cadastros para descontos, como aqui demonstrado.

2.2 Percepções dos(as) usuários(as) dos serviços de saúde digital sobre proteção de dados pessoais

Nota-se haver consenso entre os entrevistados sobre o uso de tecnologias, enquanto algo extremamente positivo em sua rotina de saúde. Mas existem também diferenças expressivas no tipo de uso que fazem das tecnologias e quais tecnologias são usadas.

Entre as perguntas feitas aos entrevistados, indagou-se especificamente sobre o uso de aplicativos de saúde e telemedicina. O primeiro parece ter extrema popularidade entre os(as) usuários(as), considerando que 87,5% das pessoas afirmaram usar ou já ter usado aplicativos de saúde (gráfico 3). Observou-se que eles usam, sobretudo, os aplicativos de contagem de carboidratos.

Gráfico 3 - Uso de aplicativos de saúde e telemedicina

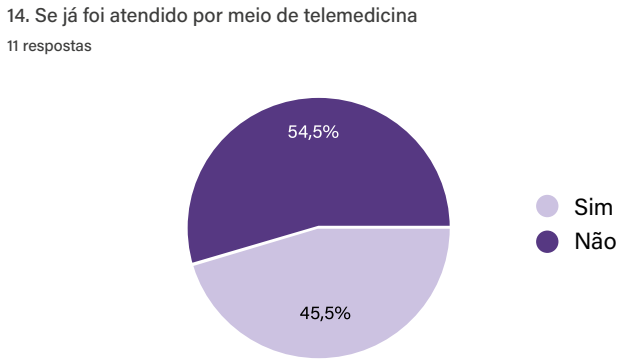


Para fins de construção de um inventário de tecnologias digitais da informação e comunicação que coleta dados pessoais sensíveis em serviços de saúde no âmbito da pesquisa "Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil", as tecnologias, os aplicativos, os dispositivos citados foram distribuídos em sete categorias, das quais cinco se mostraram relevantes para uma análise em profundidade, são elas: dispositivos portáteis de saúde, gestão integrada de informação em saúde, sistemas de apoio à decisão em saúde, plataformas utilizadas para telessaúde, plataformas utilizadas para automonitoramento.[60]

60 Essa conceituação, bem como a análise relacional entre os conceitos aqui descritos, está disponível no relatório final da pesquisa "Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil".

Com relação à telemedicina, o uso foi menos expressivo, com 45,5% das pessoas afirmando que já utilizaram o recurso, sobretudo, no período da pandemia (gráfico 4).

Gráfico 4 - Atendimento por telemedicina



O destaque, de fato, ficou para os dispositivos portáteis de saúde, que no caso dos pacientes com diabetes parece ser um diferencial de grande importância no tratamento. Embora não tenha sido formulada nenhuma questão quantitativa, nesse sentido, observou-se a forte presença deles na vida dos(as) pacientes que os utilizam e no desejo daqueles(as) que ainda não o fazem.

As tecnologias digitais, os aplicativos e os dispositivos portáteis de saúde tiveram destaque importante na compreensão de como os dados de usuários(as) circulam, a partir dessas tecnologias. Se, por um lado, a circulação de dados pessoais gera benefícios, em termos de controle da doença para usuários(as), é esse mesmo aspecto que inspira uma preocupação com relação à segurança de dados. Ao falar sobre a rotina de cuidados com a saúde, uma das usuárias conta sobre o compartilhamento de suas medições de glicose com familiares:

> Os dois aplicativos, hoje em dia, que eu realmente uso são os do Libre, de leitura, porque hoje não preciso nem usar o leitor do glicosímetro. Eu consigo ler com o meu celular a minha glicemia. Isso para mim é muito mais fácil. E uso o Libre Link, que é o de leitura. E a Abbott tem outro aplicativo do Libre que, por exemplo, o meu namorado baixou no celular dele. Se eu medir aqui, ele recebe a minha glicemia, onde ele estiver. A minha mãe, que mora em Niterói, recebe minha glicemia. Eu já recebi mensagem da minha mãe: "Está tudo bem? Está com hipo. Já

> comeu alguma coisa?". É um aplicativo do Libre, que é mais para você acompanhar. E isso eu achei sensacional porque: uma mãe que manda o filho para a escola. Alguém leu a glicemia da criança na escola? A mãe está recebendo no celular dela. Está esperando ali, se mantendo aliviada. (Usuária influenciadora digital, 35 anos, Rio de Janeiro – RJ)

2.3 Percepções dos(as) usuários(as) dos serviços de saúde digital dos riscos e das vulnerabilidades associados à coleta e ao tratamento de seus dados pessoais

Ao serem indagados sobre a preocupação com a segurança de seus dados pessoais, a maior parte dos entrevistados respondeu que se preocupa, como pode ser observado no gráfico a seguir (5). Entretanto, ao serem indagadas especificamente sobre os instrumentos de consentimento para o uso dos dados, a partir dos quais teriam registrado estar de acordo, em geral as pessoas não se recordam deles. Tampouco declararam ter uma lembrança precisa sobre o tipo de dado solicitado por serviços de saúde, farmácias, aplicativos e outros.

Como ressalta uma das usuárias:

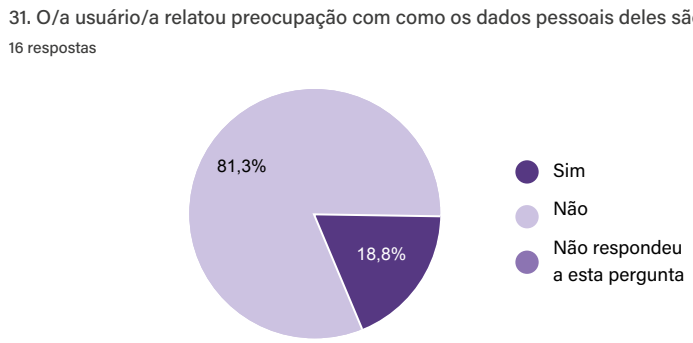
> Eu acho que a tecnologia tem tudo de benefício, só que tenho a impressão que desandou um pouco. Não tenho certeza se volta, se conseguimos fazer um retrocesso disso. Acho que não. É muito benéfico, você baixa o aplicativo e consegue comprar coisas muito facilmente por meio dele. Por exemplo, consigo falar com o meu médico. Ele me manda tudo que eu preciso fazer de exames. Ele me envia digitalmente. Eu consigo mandar o resultado dos exames para o médico. Então, você consegue fazer várias coisas, tudo *on-line*, tudo digital. No entanto, a impressão que eu tenho é que esse benefício tem um valor, tem um preço. O preço é esse mesmo, nós estarmos com os nossos dados todos aí. (Usuária da associação, 50 anos, São Paulo – SP)

Em outro relato, destaca-se mais um aspecto que se refere à circulação dos dados:

> Nós vemos os nossos dados realmente distribuídos em diversas instituições. Às vezes, recebemos um *e-mail* em que está alguma informação nossa, sendo que nunca tivemos um acesso direto naquele local. Então, isso é realmente uma questão que

preocupa, essa distribuição dos dados. (Usuária da associação, 42 anos, São Paulo – SP)

Gráfico 5 - Preocupação dos(as) usuários(as) em relação aos seus dados

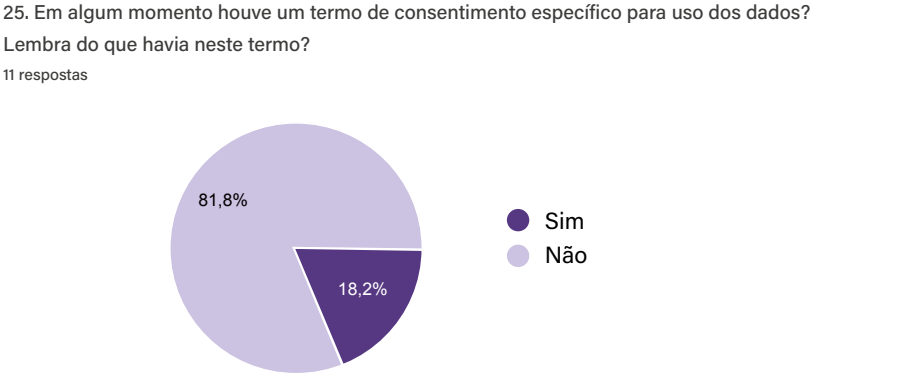


Entre os itens que os(as) usuários(as) recorrentemente se lembram de constar nos cadastros, estão:

- nome;
- idade;
- CPF;
- número da carteirinha (convênio médico);
- impressão digital (biometria);
- contato;
- endereço;
- *e-mail*;
- telefone;
- data de nascimento;
- médico responsável;
- data de quando descobriu o diagnóstico.

Uma das questões levantadas com os(as) usuários(as) foi acerca da lembrança que eles teriam sobre os termos que assinaram ou com os quais concordaram. A esmagadora maioria afirmou que não se lembra disso, como demonstrado no gráfico a seguir (6).

Gráfico 6 - Termo de consentimento para uso dos dados



A pouca lembrança ou quase nenhuma sobre esse momento se liga, sobretudo, à urgência das demandas de saúde, à necessidade de se obter um medicamento com desconto e ao modelo dos termos de privacidade que raramente são lidos pelas pessoas. Como relata uma das usuárias:

> Mais de uma vez, fiz cadastro em laboratório, não para insulina, mas para algum produto dermatológico, às vezes o próprio funcionário da farmácia pergunta: "Você tem o desconto do laboratório? Nós fazemos agora, se quiser". Depois, ele faz e não me informa nada sobre isso. Ele aceita tudo, pede os dados que precisa e pronto, estou cadastrada. Quando faço em casa, há o espaço para você clicar, dizendo se você concorda com os termos de privacidade, e, sendo bem sincera, eu nunca leio, só concordo e seja o que Deus quiser. (Usuária da associação, 50 anos, São Paulo – SP)

Esses relatos revelam que a preocupação existe entre boa parte dos(as) usuários(as), porém, na maior parte das vezes, materializar essa preocupação em ações concretas de proteção é difícil, já que os(as) usuários(as) não conhecem exatamente o fluxo e o funcionamento do mercado de dados pessoais.

As perguntas que questionavam sobre formas de armazenamento e tratamento de dados, em sua ampla maioria, foram respondidas com apenas um "não", "não tenho ideia" ou um aceno negativo com a cabeça. Em alguns casos, alguma ideia ainda bastante difusa tentava ser formulada. Por exemplo, quando perguntamos sobre

quem seriam as pessoas, os órgãos ou os agentes que teriam acesso aos dados, essas foram algumas das respostas:

> Atendimento que pega os dados. Pessoa que vai colocar os dados nos bancos de dados. Uma vez que os dados estejam no banco de dados.
>
> Eu imagino que seja o pessoal de TI, ou o pessoal do setor administrativo da empresa, mas é só a minha impressão.
>
> Não. Eu imagino que os médicos que eu passo, mas além deles, não faço a mínima ideia.
>
> Agentes da saúde.

Em uma pergunta no mesmo sentido, usuários(as) foram indagados sobre as formas de registro e armazenamento de seus dados e as respostas apontam para a mesma vaga percepção da pergunta anterior.

> Eu acho que são armazenados em servidores, o meu e de milhões de brasileiros, para pesquisa deles.
>
> Arquivados, armazenados em algum banco de dados, e talvez através desse banco de dados os meus dados são utilizados para fazer alguma tabela de Excel, algum levantamento de dados de usuários, coisas assim.
>
> Nunca parei para pensar sobre isso. Eu imagino que em uma plataforma da própria empresa, para armazenamento de dados. Como um Excel diferenciado.
>
> Eu sou da época do arquivo morto, acho que passou vai para o arquivo morto (rindo). Vai para nuvem (escura), vai para nuvem cheia de água, sei lá, não sei, assim, te dizer. Imagino, assim, sabe aquela coisa antiga dos arquivos?
>
> Eu não consigo imaginar essa danada dessa nuvem tão grande que consegue ir tanta gente, tantos dados, mas como tenho um filho que faz engenharia de computação, ele me dá alguma informação dos provedores. E todos esses cadastros são feitos via provedores e internet. Na verdade, esses dados que são, digamos assim, como foi que ele disse, ele disse que os dados eram utilizados, eram desmembrados para diversos setores que tinham interesse.

> Não faço ideia. Embora trabalhe com a área da tecnologia, só sei que fica em algum servidor. São vendidos esses dados. Isso é certeza.

Com base nas respostas dos(as) usuários(as), podemos nos indagar sobre como podemos construir uma cultura de proteção de dados pessoais entre agentes que atuam na saúde, considerando que os(as) usuários(as) não estão inseridos em um contexto em que a proteção da privacidade e dos dados pessoais é afirmada como um direito e garantida pelo Estado. Como falar em uma cultura de proteção de dados pessoais, quando a preocupação dos(as) usuários(as) com os riscos aos quais estão submetidos(as) pela circulação de seus dados não são acompanhados, por um lado, de mecanismos de transparência que ofereçam as informações necessárias sobre o mercado de dados pessoais e, por outro lado, de regulação e fiscalização por parte do Estado?

Considerações finais

Como vimos na abertura deste texto, o Brasil é um país com um marco regulatório atual sobre internet e proteção de dados pessoais. No entanto, observam-se alguns limites e barreiras para a incorporação de direitos digitais, de uma forma geral, por parte da população e, nesse caso, principalmente, por parte da população mais vulnerável, cujo acesso ao ambiente digital e às tecnologias, como já foi dito, é restrito e desigual.

Esse trabalho buscou, a partir de um direito social fundamental e incorporado pela população, que é o direito à saúde, observar a percepção de um outro direito que emerge como fundamental, que é o direito à proteção de dados pessoais. Buscou-se também fazer essa relação, a partir do direito à informação e à comunicação, que avaliamos ser fundamental para compreensão, apropriação e fortalecimento tanto do direito à saúde quanto da proteção de dados pessoais.

A partir dessas conexões, a pesquisa buscou entender percepções sobre a proteção de dados pessoais com base no que a LGPD considera dados pessoais sensíveis, dados que têm um potencial de interferir na vida e na privacidade do(a) cidadão(ã) e que, portanto, são regidos por disciplinas ainda mais rígidas e cuidadosas. Embora, como dissemos no início desse artigo, a lei considere os dados de saúde como dados sensíveis, não há ainda uma regulamentação precisa sobre quais dados são considerados de saúde, visto que cada vez mais informações relacionadas aos nossos hábitos de consumo e lazer são coletadas cotidianamente e falam sobre os nossos estilos de vida e da saúde numa concepção ampliada.

Além disso, cabe ser discutido que dados pessoais coletados são realmente necessários para o desenvolvimento das tecnologias em saúde ou se a coleta de dados extrapola esses objetivos, em nome de outras finalidades de uso. A ausência de transparência e a falta de controle público dificultam a análise dessa questão e a tornam ainda mais opaca para os(as) usuários(as). Atrelado a isso, seria importante também indagarmos que benefícios os(as) usuários(as) recebem em troca do fornecimento de seus dados pessoais, tanto em nível individual quanto em nível coletivo, com relação ao desenvolvimento da saúde pública.

Deve-se atentar para a lenta implementação da ANPD como um dos problemas e gargalos para a resolução das questões que surgem a partir da vigência da lei – como, por exemplo, as definições infralegais do que venham a ser, de fato, dados de saúde –, e também da própria fiscalização sobre a adequação do tratamento de dados pessoais por empresas que coletam e tratam dados em escala e velocidade imensuráveis. Para além disso, caberia também à ANPD, junto aos órgãos estatais, atuar na construção de estratégias para uma cultura de proteção de dados pessoais que considerasse a realidade e as demandas da sociedade brasileira.

Ao fazer o levantamento bibliográfico para fins da pesquisa "Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil", da qual este capítulo é subsidiário, observou-se, por exemplo, que o(a) usuário(a) para o(a) qual a proteção de dados pessoais se destina é um sujeito quase inexistente nas pesquisas analisadas. Entende-se, portanto, ser difícil construir uma cultura de proteção de dados pessoais que não seja uma repetição de padrões estabelecidos em outros contextos, sem saber o que os(as) diferentes usuários(as) brasileiros(as) pensam sobre isso, o que, afinal, entendem por proteção de dados pessoais.

Dessa forma, buscou-se ouvir, ainda que de forma preliminar e exploratória, o(a) usuário(a), entre outras coisas, para compreender a sua percepção sobre o tema e buscar inferir caminhos e horizontes a serem percorridos para pensarmos os desafios de uma cultura de proteção de dados pessoais que reflita a realidade local e responda aos problemas reais de um país considerado periférico. Essa discussão não pode ignorar a lógica global de fluxo de dados transfronteiriço em que até mesmo os direitos dos(as) usuários(as) à proteção dos seus dados pessoais variam de acordo com o *status* do país na hierarquia das economias mundiais, criando categorias diferentes de cidadãos(ãs) quanto à garantia de proteção de dados pessoais.

Ao analisarmos as 16 entrevistas em profundidade trazidas neste texto, pode-se observar que, de uma maneira geral, há, para além da percepção dos benefícios das tecnologias da informação e da comunicação aplicadas à saúde, um receio

quanto ao compartilhamento de dados pessoais, principalmente, quando feito por meio de plataformas digitais, aplicativos de automonitoramento e de telessaúde e também nas farmácias.

De forma geral, o(a) usuário(a) entende que há questões não nítidas envolvidas na coleta de dados no dia a dia – algo cada vez mais constante. Chama a atenção do(a) usuário(a), por exemplo, o acesso às informações, inclusive as relacionadas à saúde, de empresas com as quais eles nunca compartilharam os seus dados. Isso, claro, gera dúvidas sobre como essas empresas têm acesso aos dados não compartilhados ou não autorizados para esse fim e cria uma sensação de impotência e irreversibilidade frente à atual situação de perda de controle sobre o fluxo dos seus dados. Muitos relatos demonstram um conformismo diante da situação de perda total de controle de seus dados e com a qual seria impossível "lutar contra", já que "não haveria mais" condições de reaver o controle.

Para além da percepção do risco, quando temos o compartilhamento *versus* a necessidade de aderir aos programas de desconto, observou-se que falta também informação e conhecimento sobre os fluxos dos dados coletados (quem coleta, se e como trata, se e com quem compartilha, por exemplo), sobre os possíveis riscos do uso daqueles dados, bem como as finalidades para as quais os dados são coletados. Essa ausência de informações, como descreve a lei, dificulta uma possível equação sobre o consentimento do uso dos dados pessoais na saúde. A grande maioria dos entrevistados, inclusive, afirmou não ler ou não lembrar do que dizem os termos de uso dos aplicativos, das plataformas e dos dispositivos utilizados.

Outra camada que pudemos observar são as desigualdades no acesso às tecnologias em saúde. Há as desigualdades sociais que geram acessos desiguais às tecnologias, de uma forma geral, dificultando o gozo de benefícios por uma parte menos favorecida da população. Mas essas desigualdades também são responsáveis por uma maior vulnerabilidade de determinados grupos, podendo ampliar riscos associados a possíveis discriminações que o acesso às tecnologias também trazem. Em algumas situações, os grupos mais vulneráveis e que geralmente têm menor acesso aos benefícios, têm também maior impacto dos riscos.

Estudos sobre o uso de algoritmos e de Inteligência Artificial (IA) no tratamento de dados pessoais e de imagens têm revelado riscos latentes. Segundo Silveira e Silva (2020), há uma relação entre falta de transparência dos sistemas algorítmicos e processos discriminatórios de pessoas e segmentos da população, quando submetidos à governança praticada pelos algoritmos.

Essa realidade corrobora com o entendimento de que o(a) usuário(a) não pode ser visto como o principal responsável pela mitigação dos riscos associados ao compartilhamento de seus dados pessoais. Existe uma assimetria das relações entre os agentes que coletam e usam os dados pessoais (indústria farmacêutica, grandes plataformas, redes de farmácias etc.) e os(as) cidadãos(ãs).

A partir de duas noções trabalhadas nesse texto – a noção de uma cultura de proteção de dados pessoais e a de uma assimetria informacional –, compreende-se que o fortalecimento da proteção de dados pessoais, como um direito, exige a presença dos(as) usuários(as), enquanto sujeitos de pesquisa, e também da participação deles nos espaços públicos de debate sobre o tema, pensando especificamente nas políticas públicas em saúde no que tange à informação.

Diante desse diagnóstico, entende-se que o Estado é o principal ente capaz de, em primeira instância, garantir os direitos digitais dos(as) usuários(as), incluindo a proteção de dados pessoais frente às grandes corporações, seus lucros e ao mercado indiscriminado de dados pessoais. Falar, portanto, de cultura de proteção de dados pessoais é falar de marcos legais que deem subsídios às políticas, mas também de políticas públicas setorizadas e efetivas. Tais políticas precisam colocar o(a) cidadão(ã) e os seus dados pessoais na condição de sujeitos protegidos frente ao avassalador e crescente mercado de dados impulsionado por *Big Techs* que transitam entre os setores do entretenimento, do comércio e da saúde sem grandes barreiras.

Um rol de dados inegociáveis, a fiscalização do compartilhamento de dados sensíveis entre empresas e marcas de uma mesma empresa, que atuem em áreas diferentes ou com conflitos de interesse, bem como a regulação do funcionamento das plataformas que não apenas coletam dados, mas também são capazes de predizer comportamentos, são fundamentais para a construção de uma cultura de proteção de dados baseada em aspectos reais e que coloquem os sujeitos em condições de garantia e proteção de seus direitos, assim como acontece, ou deveria acontecer, em outros campos dos direitos fundamentais.

Referências

ABU-LUGHOD, Lila *et al.* A escrita contra a cultura. **Equatorial: Revista de Programa de Pós-graduação em Antropologia Social**, v. 5, n. 8, p. 193-226, 2018. Disponível em: https://periodicos.ufrn.br/equatorial/article/view/15615. Acesso em: 20 jan. 2024.

APPADURAI, Arjun. The Production of Locality. *In*: FARDON, Richard. (ed.). **Counterworks**: Managing the diversity of knowledge. Londres: Routledge, 1995. p. 204-225.

BELLI, Luca; DONEDA, Danilo. O que falta ao Brasil e à América Latina para uma proteção de dados efetiva?. **Jota**, 2 set. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-que-falta-ao-brasil-e-a-america-latina-para-uma-protecao-de-dados-efetiva-02092021. Acesso em: 9 ago. 2022.

BRASIL. Presidência da República. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei n. 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 fev. 2022.

CLIFFORD, James. **The predicament of culture**: Twentieth-Century Ethnography, Literature, and Art. Cambridge: Harvard University Press, 1988.

COALIZÃO DIREITOS NA REDE. Vitória! Senado Federal aprova projeto de Lei Geral de Dados Pessoais. 11 jul. 2018. Disponível em: https://direitosnarede.org.br/2018/07/11/vitoria-senado-aprova-lgpd/. Acesso em: 18 jul. 2022.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2, p. 91-108, jul.-dez. 2011. Disponível em: file:///C:/Users/maria/Desktop/Dialnet-AProtecaoDosDadosPessoaisComoUmDireitoFundamental-4555153.pdf. Acesso em: 2 nov. 2021.

HANNERZ, Ulf. Fluxos, fronteiras, híbridos: palavras-chave da antropologia transnacional. Mana: Estudos de Antropologia Social, v. 3, n. 1, p. 7-39, abr. 1997. DOI: https://doi.org/10.1590/S0104-93131997000100001. Disponível: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.scielo.br/j/mana/a/bsg6bwchcBbqfnpW6GYvnPg/?format=pdf&lang=pt. Acesso em: 10 jan. 2024.

INTERVOZES. Relatório Direito à Comunicação no Brasil 2022. São Paulo: Intervozes, 2023. Disponível em: https://app.rios.org.br/index.php/s/jm9CTxtQ4wMbgQx. Acesso em: 10 jan. 2024.

LINKE, Sarah Helena. Sociedade de vigilância e consumo: proteção de dados pessoais relacionados à saúde em programas de fidelização de redes de

farmácia. Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Federal de Santa Catarina, 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 469-483, Revista dos Tribunais, nov.-dez. 2018.

QUIJANO, Aníbal. Colonialidade do poder, eurocentrismo e América Latina. *In*: LANDER, Edgardo. (Org.). **A colonialidade do saber**: eurocentrismo e ciências sociais. Perspectivas latino-americanas. Buenos Aires: CLACSO, Consejo Latinoamericano de Ciencias Sociales Editorial, 2005. Colección Sur Sur. p. 107-130.

RODOTÀ, Stefano. **A vida na sociedade de vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SILVA, Gabriela B. P.; MODESTO, Jessica A.; JÚNIOR, Marcos E. O tratamento de dados no combate à covid-19: dilemas entre o interesse público e o direito à privacidade na Lei Geral de Proteção de Dados Pessoais. **Revista Jurídica Luso-Brasileira (RJLB)**, ano 6, n, 6, p. 571-609, 2020. Disponível em: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cidp.pt/revistas/rjlb/2020/6/2020_06_0571_0609.pdf. Acesso em: 8 jan. 2024.

SILVA, Tarcizio; SILVEIRA, Sérgio. Controvérsias sobre dados algorítmicos: discursos corporativos sobre discriminação codificada. in **Revista Observatório,** V. 6 Nº 4 (2020) **Disponível em:** https://sistemas.uft.edu.br/periodicos/index.php/observatorio/article/view/11071/17865. Acesso em: 5 jan. 2024

SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. *In*: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da. **Colonialismo de dados**: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, 2021. p. 41-42.

SILVEIRA, Sérgio Amadeu da; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc em Revista**, v. 12, n. 2, 2016. DOI: https://doi.org/10.18617/liinc.v12i2.902. Disponível em: https://revista.ibict.br/liinc/article/view/3719. Acesso em: 5 jan. 2024.

THOMPSON, John B. I**deologia e cultura moderna**: teoria social crítica na era dos meios de comunicação de massa. Petrópolis: Vozes, 1995.

VAN DIJCK, José; POELL Thomas. Understanding the promises and premises of online health platforms. **Big Data & Society**, v. 3, n. 1, jan.-jun. 2016. DOI: https://doi.org/10.1177/2053951716654173. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/2053951716654173. Acesso em: 5 fev. 2024.

WESTRUP, Ana Carolina. Lei Geral de Proteção de Dados não impede o vazamento de dados pessoais. **Le Monde Diplomatique Brasil**, 19 maio 2022. Disponível em: https://diplomatique.org.br/lei-geral-de-protecao-de-dados-nao-impede-o-vazamento-de-dados-pessoais/. Acesso em: 18 jul. 2022.

WILLIAMS, Raymond. **Cultura e sociedade**: de Coleridge a Orwell. Petrópolis: Vozes, 2011.

WILLIAMS, Raymond. **Marxismo e literatura**. Rio de Janeiro: Zahar, 1979.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira de poder. 1. ed. Rio de Janeiro: Intrínseca, 2021.

https://doi.org/10.29397/EdicoesLivres/20250111

Riscos e vulnerabilidades à proteção de dados pessoais em um contexto de digitalização dos serviços de saúde

Fabiana Dias

Este capítulo apresenta reflexões sobre os riscos e as vulnerabilidades à proteção de dados pessoais nos contextos da saúde digital e do uso crescente das Tecnologias da Informação e Comunicação (TICs) na saúde. Teve como referência e base de dados a pesquisa Proteção de Dados Pessoais em Serviços de Saúde Digital realizada pelo Instituto de Comunicação e Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz), pelo Intervozes – Coletivo Brasil de Comunicação Social e pelo Instituto Brasileiro de Defesa de Consumidores (Idec), com o objetivo de fortalecer a cultura de proteção de dados pessoais na área da saúde, tendo como referência a Lei Geral de Proteção de Dados Pessoais (LGPD).

O uso das TICs está cada vez mais presente no cotidiano, incluindo as relações de trabalho, lazer e a interação entre as pessoas, por meio do acesso aos recursos tecnológicos via celular ou computador. A globalização, como um fenômeno de integração econômica, social e cultural em escala mundial, tem contribuído para difundir esse processo (Stevanim; Murtinho, 2021; Silva; Marques, 2011).

Na área da saúde, as TICs têm sido utilizadas principalmente na gestão do cuidado por meio dos Registros Eletrônicos de Saúde (RES), como o prontuário eletrônico e outros sistemas de informação informatizados, o que tem gerado o compartilhamento das informações dos usuários entre profissionais, gestores, prestadores de serviços e outros agentes que compõem a cadeia de coleta e tratamento dos dados pessoais nos serviços de saúde.

Com o avanço da saúde digital, temos observado a ampliação da produção de dados, o armazenamento e a circulação de informações da vida privada dos cidadãos (Stevanim; Murtinho, 2021). Esse cenário evidencia a necessidade da implementação de medidas destinadas à segurança da informação e à instituição de boas práticas no manuseio dos dados de saúde, de modo a garantir a proteção dos dados pessoais dos usuários, assim como a privacidade e a confidencialidade desses dados.

Cabe destacar que a proteção de dados não pretende impedir a circulação e o tratamento da informação, mas, sim, estabelecer os parâmetros para a sua realização. Sob esse aspecto, é importante garantir a privacidade, que diz respeito ao resguardo da intimidade e da vida privada do indivíduo, e a confidencialidade, que está relacionada à preservação das informações privadas e íntimas, fornecidas em confiança, e à proteção contra a sua revelação não autorizada (Stevanim; Murtinho, 2021; Goldim, 2024).

Na perspectiva da proteção de dados pessoais, tivemos a promulgação da LGPD (lei n. 13.709/2018), que entrou em vigor em setembro de 2020 e que dispõe sobre as regras, os princípios, os direitos e os deveres dos cidadãos, de forma que as pessoas possam questionar e acompanhar como os seus dados são tratados (Brasil, 2018).

Nesse sentido, a proteção de dados pessoais foi abordada neste estudo como um direito à informação e à comunicação, sobretudo devido a sua associação a outros direitos, tais como o direito à saúde. O reconhecimento e a garantia desses direitos são fundamentais para reduzir as iniquidades e promover as transformações sociais necessárias para a qualidade de vida e o bem-estar mais democrático das populações, estando intimamente relacionados ao exercício pleno da cidadania (Brasil, 2015).

Ao considerarmos o uso das soluções digitais nos serviços públicos e privados de saúde, é importante problematizar e refletir sobre os avanços e desafios inerentes à saúde digital, visto que, ao mesmo tempo que as tecnologias trazem benefícios, como a otimização dos fluxos de atendimento, a vigilância em saúde e a eficácia de tratamentos, elas podem também criar novos problemas a serem enfrentados.

Dessa forma, de modo a realizar uma reflexão crítica sobre os riscos e as vulnerabilidades à proteção de dados pessoais, nos serviços de saúde, este texto foi organizado em três partes. A primeira seção buscou contextualizar e apreender discussões sobre a saúde digital e a proteção de dados na realidade dos serviços. A seção seguinte apresenta brevemente os marcos legais e normativos relevantes que advogam a proteção de dados pessoais como um direito do cidadão. Na parte final, o texto apresenta uma análise crítica e reflexiva sobre os riscos e as vulnerabilidades à proteção de dados pessoais identificados por meio da revisão bibliográfica que foi uma das estratégias metodológicas da pesquisa.

1. A saúde digital e a proteção de dados pessoais

Ao contextualizar a digitalização dos serviços de saúde, é necessário considerar alguns aspectos históricos relacionados ao tema ao longo do tempo. E, nesse sentido, é importante destacar que a transformação digital observada mundialmente tem relação com o advento da Sociedade da Informação que, segundo Castells (1999), se caracterizou como um período histórico marcado por uma revolução tecnológica mediada pelas tecnologias digitais de informação e comunicação, difundidas em diversos países, principalmente sob o efeito da globalização e das políticas neoliberais. Essa revolução acelerou os processos de interação entre os indivíduos e as organizações de modo a gerar uma sociedade informacional e um sistema econômico mundial, fomentando, assim, a expansão e a reestruturação do capitalismo, principalmente, com o surgimento da internet (Borges; Gomberg; Borges, 2019).

Nessa nova configuração social, as TICs tiveram um papel primordial em um cenário marcado por alterações técnicas, organizacionais e administrativas. Esse processo possibilitou a propagação da digitalização dos serviços no campo da saúde, o que vem sendo denominado de saúde digital.

O conceito de saúde digital compreende as tecnologias direcionadas a entregar cuidados de saúde, prover informações e compartilhar experiências de saúde e doença (Lupton, 2017). Como exemplos dos recursos tecnológicos utilizados, temos os computadores, o uso da internet, os prontuários eletrônicos e os sistemas informatizados para o agendamento de consultas, exames e cirurgias, a realização de atendimentos, o registro de notificações em saúde, a construção de bancos de dados, o armazenamento e a recuperação de informações dos usuários.

A digitalização da saúde também tem sido difundida por organismos internacionais, como a Organização Mundial da Saúde (OMS). A OMS, por meio da Estratégia Global de Saúde Digital, tem fomentado a colaboração entre os países, a troca de conhecimentos e de experiências entre os centros de pesquisa, as empresas, as organizações de saúde e as associações de usuários, com a justificativa de promover a saúde para todos e em todos os lugares (OPAS, 2019).

No Brasil, a Estratégia de Saúde Digital (ESD) faz parte desse movimento e tem sido implementada pelo Ministério da Saúde, de modo a produzir e disponibilizar informações sobre saúde em tempo oportuno (Brasil, 2017). Um dos programas vinculados a essa estratégia e com grande repercussão durante a pandemia da covid-19 foi o Conecte SUS, uma iniciativa que teve como objetivo priorizar as ações de alinhamento frente às necessidades nacionais de combate à pandemia.

A pandemia da covid-19 deu uma maior visibilidade à utilização das TICs de modo a gerar informação e comunicação na perspectiva da saúde e subsidiar as tomadas de decisão. Ao mesmo tempo, evidenciou os riscos e as vulnerabilidades atrelados aos sistemas de informação no que tange à segurança, à privacidade e à confidencialidade dos dados de saúde frente a uma emergência de saúde pública e diante da necessidade de acesso e compartilhamento de dados de saúde entre os agentes governamentais e as instituições de pesquisa e saúde.

Nesse período, ocorreu o vazamento de senhas do Ministério da Saúde por meio da publicação de uma planilha em uma plataforma aberta de compartilhamento de códigos de programação e arquivos que permitiu o acesso a dados como CPF, telefone e doenças preexistentes de 16 milhões de pessoas em todo o país com diagnóstico confirmado ou suspeita de covid-19. Na ocasião, o arquivo contendo as senhas foi publicado sem a proteção adequada em decorrência de um projeto firmado entre o Ministério da Saúde e uma instituição privada de saúde (Salim, 2021).

Outro fato evidenciado e relacionado ao serviço de saúde de forma remota foi a desigualdade no acesso às tecnologias, visto que parcela significativa da população não tem acesso à rede de internet. De acordo com a ONU (2020), a população mundial que não tem acesso à internet está em uma terrível desvantagem, não só no acesso à informação, mas no acesso à educação, aos dados sobre saúde, às possibilidades de trabalho e às formas de compensar a crise econômica – o que acentua, sem dúvida, as desigualdades sociais.

A pandemia também oportunizou a problematização de temas sensíveis, como a prática de telemedicina, a prescrição eletrônica de medicamentos e a proteção de dados pessoais diante da utilização de um grande volume de dados, seja no sistema público ou privado de saúde, suscitando discussões quanto às questões éticas e legais da LGPD em relação a esse contexto.

A LGPD 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 (Brasil, 2018).

Com a expansão do uso de dados pessoais na área da saúde, foi possível observar que a produção de conhecimento a respeito do tema saúde digital e proteção de dados pessoais ainda é insuficiente para nortear a atuação de organizações públicas e privadas e, ao mesmo tempo, possibilitar a adequação das práticas dos serviços digitais ao ecossistema legal de proteção de dados.

Da mesma forma, ainda são insuficientes as referências de boas práticas para a coleta e o tratamento de dados pessoais de saúde, bem como os materiais de referência e produtos de comunicação sobre os direitos dos usuários à proteção de dados pessoais (Icict/Fiocruz; Idec; Intervozes, 2022).

Tal constatação reforça a relevância da pesquisa Proteção de Dados Pessoais em Serviços de Saúde Digital para as políticas públicas, sobretudo no que diz respeito aos direitos de cidadania, visto que a proteção de dados pessoais está associada ao direito à saúde, à comunicação e à informação. Para a efetivação desses direitos é imprescindível uma melhoria no sistema de saúde no tocante à cultura de proteção de dados.

2. O direito à proteção de dados pessoais

A proteção de dados pessoais no Brasil foi recentemente reconhecida enquanto um direito fundamental por meio da emenda constitucional n. 115 de 2022 (Brasil, 2022), acrescentando ao artigo 5º da Constituição Federal o inciso LXXIX, que assegura, nos termos da lei: "[...] o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Esse reconhecimento foi posterior à Proposta de Emenda à Constituição n. 17 de 2019 (PEC 17/2019) que propôs a inclusão da proteção de dados pessoais entre os direitos e as garantias fundamentais na Constituição Federal e a União como o órgão de competência privativa para legislar sobre a proteção e o tratamento de dados pessoais (Brasil, 2019; 2022).

Cabe destacar que a centralização da legislação sobre o tema na União tem gerado divergências ao atribuir essa competência privativa a apenas um dos entes federativos, gerando questionamentos sobre a autonomia constituinte dos estados, visto que outras normas do sistema constitucional podem ser impactadas, principalmente nos casos de conflitos federativos nas situações de leis transversais como as observadas nos serviços de telecomunicações, trânsito e transportes (Quintiliano, 2021).

O direito dos cidadãos à proteção de dados pessoais vem sendo discutido mundialmente e incidindo na instituição de estratégias normativas e legais de proteção da vida privada diante da digitalização que, ao mesmo tempo em que oferece oportunidades, gera ameaças, já que temos acompanhado o aumento do uso abusivo ou indevido dos dados pessoais, além de acentuar a vulnerabilidade do direito à intimidade (Carvalho, 2019).

Quanto aos instrumentos normativos legais, eles têm se tornado essenciais e indispensáveis para a proteção jurídica à privacidade fundamentada no princípio constitucional da dignidade humana, principalmente quando se trata de questões de saúde. Destaca-se também o potencial risco discriminatório que o vazamento total ou parcial da informação sobre a saúde das pessoas pode trazer frente aos impactos sociais, econômicos e políticos originários dos avanços tecnológicos (Sarlet; Keinert, 2015; Pinheiro, 2018).

Por conseguinte, o surgimento desses regramentos também tem sido resultado da associação entre a expansão dos direitos humanos e a atualização e a adaptação de documentos internacionais de proteção aos direitos (Sarlet; Keinert, 2015; Pinheiro, 2018).

A LGPD foi um marco na regulamentação de dados pessoais no país ao discorrer sobre todas as operações de tratamento de dados, inclusive, as dos meios digitais. É importante frisar a necessidade do consentimento do usuário para a coleta e o tratamento dos dados visto o seu direito à propriedade dos dados, ainda que estejam sob a guarda dos serviços de saúde.

Todavia, em algumas situações de emergência e de interesse público, como a saúde pública, o uso de dados pessoais é permitido, mesmo sem o consentimento do seu titular, fazendo-se necessário que haja salvaguardas e proporcionalidade no uso dos dados para o alcance das finalidades e especificidades referentes às credenciais dos órgãos autorizados a processar os dados (Brasil, 2018).

A adequação aos marcos normativos e legais demanda o uso de tecnologia, infraestrutura e pessoal qualificado para que os dados sejam tratados de forma lícita, justa e responsável em relação aos titulares dos mesmos, em consonância ao princípio da responsabilização e do acompanhamento das atividades de processamento pelas autoridades designadas, que poderão aplicar sanções, quando houver descumprimento da lei (Doneda, 2019).

Ressalta-se que a garantia legal é uma condição necessária para o exercício de um direito, mas não é suficiente, o que demanda lutas sociais permanentes para a sua efetivação (Stevanim; Murtinho, 2021).

A governança responsável dos dados deve ser pautada na transparência e no empoderamento dos cidadãos para que haja confiança e estabelecimento de relacionamentos equilibrados e justos entre indivíduos e organizações.

3. Riscos e vulnerabilidades à proteção de dados pessoais nos serviços de saúde

Diante das preocupações quanto à segurança da informação e à proteção dos dados pessoais em um contexto de desenvolvimento tecnológico, serão aqui apresentados e discutidos os resultados obtidos em relação aos riscos e às vulnerabilidades à proteção de dados pessoais nos serviços de saúde, públicos ou privados, identificados por meio de uma revisão bibliográfica.

A revisão foi realizada nas bases de dados da Biblioteca Virtual em Saúde (BVS), do Oasisbr[1] e do Google Acadêmico. As buscas compreenderam o período de 2014 a 2021, tendo como referência temporal o Marco Civil da Internet (MCI) que estabelece os princípios, as garantias, os direitos e os deveres para o uso da internet no Brasil, sobretudo no que se refere à privacidade, à confidencialidade e à proteção dos dados pessoais.

Após as buscas nas bases de dados, foi considerado um conjunto de 82 trabalhos científicos contemplando o tema da pesquisa. As principais áreas de conhecimento das publicações foram: ciências da saúde, ciências jurídicas, ciências da informação e comunicação e estudos na área de tecnologia e informática.

O período de 2018 a 2021 concentrou um maior número de publicações nas áreas de conhecimento supracitadas, o que pode indicar o impacto das discussões em torno da LGPD. O conjunto de estudos contemplou artigos publicados em revistas científicas, teses, dissertações, trabalhos de conclusão de curso de graduação e capítulos de livros.

Os achados provenientes das buscas nas bases de dados foram exportados para um *software* de gerenciamento de referências, Zotero, para um melhor manejo dos dados bibliográficos e materiais relacionados à pesquisa.

Entre os estudos selecionados, 78,3% foram publicados por pesquisadores de origem nacional, 19,3%, internacional e 2,4%, por pesquisadores de origem multinacional, resultando em 85,5% das publicações no idioma português, o que se justifica devido ao uso de bases de dados latino-americanas, além da maior concentração de estudos publicados por pesquisadores de origem nacional.

Em relação aos pesquisadores de origem nacional, a região Sudeste concentrou o maior percentual de publicações sobre a temática proteção de dados pessoais, com 42,2% dos pesquisadores vinculados a instituições de ensino ou grupo de

1 O Portal Brasileiro de Publicações e Dados Científicos em Acesso Aberto (Oasisbr): https://oasisbr.ibict.br/vufind.

pesquisa nessa região do país, seguida da região Sul com 28,1%, a região Nordeste com 15,6%, a região Centro-Oeste com 10,9% e a região Norte com 3,2%.

Quanto aos pesquisadores de origem internacional, 51,4% estavam vinculados a instituições de ensino ou grupo de pesquisa na América do Sul, seguido de 43,2% vinculados a instituições na Europa e 5,4% a instituições na Oceania.

A análise bibliográfica foi realizada por meio de um roteiro contendo questões relevantes ao uso das TICs na saúde, entre elas a proteção de dados pessoais nos serviços de saúde, considerando-se a instituição de práticas de segurança da informação, privacidade e confidencialidade dos dados, e a identificação dos riscos e das vulnerabilidades referentes à coleta e ao tratamento dos dados, inclusive no âmbito farmacêutico.

Outros aspectos foram considerados, tais como: os agentes envolvidos nessa prática; a participação dos usuários, profissionais e gestores nas discussões sobre a proteção de dados; além dos marcos legais e conflitos éticos no uso das informações em saúde.

A pesquisa identificou que 78,3% dos estudos que compuseram a análise fizeram menção a riscos e vulnerabilidades relacionados ao tema saúde digital e proteção de dados pessoais e trouxeram discussões pertinentes à ausência de uma política nacional de segurança dos dados – o que implica questões de regulamentação, éticas e legais quanto à coleta e ao tratamento dos dados de saúde.

Os riscos e a vulnerabilidades identificados e que serão discutidos adiante foram agrupados de acordo com os seguintes aspectos: monetização dos dados pessoais; perfilamento de comportamento; questões relacionadas à privacidade, à confidencialidade e à segurança da informação; participação dos usuários nas discussões e no acesso às informações sobre proteção de dados pessoais; e a qualificação dos agentes de tratamento dos dados.

3.1 Monetização dos dados pessoais

Segundo Aragão e Schiocchet (2020), com o crescimento exponencial da valoração de informações, o dado passou a ser um bem valioso e, a partir dessa concepção, ocorreu a transformação da informação em uma fonte de receita.

À luz dessa concepção, o estudo de Linke (2019) apontou que a monetização dos dados pessoais em saúde possibilita a criação de novas estruturas de poder, por meio de práticas relacionadas à economia da informação, correlacionando o volume de dados obtidos pelas empresas e as possibilidades de monetização

das informações sobre os seus domínios. A autora exemplifica esse argumento a partir das redes de farmácia que condicionam valores de produtos à identificação do consumidor por meio do seu CPF – os chamados programas de fidelidade – incidindo em riscos e vulnerabilidades aos usuários, visto que essa prática não se detém às estratégias de publicidade, mas faz também compartilhamentos e usos dos dados para outras finalidades que os consumidores sequer imaginam.

De acordo com Souza (2018), existe uma falta de transparência das práticas econômicas em relação aos dados pessoais, o que impede que as pessoas saibam como as suas informações estão sendo utilizadas para a monetização. E, para além da prerrogativa do uso dos dados pessoais para a melhoria das práticas de saúde, o que tem ocorrido é uma nítida monetização da vida. Isso porque, ao mesmo tempo que os dados pessoais possibilitam a pesquisa científica e o desenvolvimento de ações preventivas, promovidas pela biopolítica do Estado para melhorar a saúde da população, também servem de insumo fundamental para que as corporações e os órgãos, inseridos na economia informacional global e no capitalismo de vigilância, lucrem cada vez mais.

Ainda, segundo Souza (2018), no capitalismo de vigilância, a experiência humana torna-se a matéria-prima que será processada e mercantilizada como dados comportamentais, por meio do desenvolvimento tecnológico e da arquitetura global computacional, ambos usados nos processos de coleta, monitoramento e classificação dos dados pessoais. Isso ocorre, principalmente, com a construção de Big Data como um modelo de tratamento, base de análise e intervenção social.

Para Carvalho (2018), parte da atual problemática do uso econômico dos dados pessoais relaciona-se com a preocupação com o direito fundamental à privacidade, que se encontra em risco de violação diante das diversas práticas de tratamento desses dados, além das implicações no exercício da cidadania.

Nessa perspectiva, os estudos abordaram a monetização dos dados pessoais como um dos efeitos atrelados ao excessivo desenvolvimento tecnológico que aumentou o potencial de uso abusivo ou indevido dos dados, acentuando a vulnerabilidade do direito à intimidade.

3.2 Perfilamento de comportamento

A utilização de informações pessoais para a construção de perfis individuais ou de grupos pode ser observada em diversos contextos e para as mais diversas finalidades. A técnica de perfilamento consiste em descobrir correlações entre dados que podem ser usados para identificar e representar um indivíduo ou grupo.

Assim, esses dados são transformados em conhecimento ou inferências, que podem ser utilizados para individualizar e representar um sujeito ou para identificar um sujeito como membro de um grupo ou categoria, propiciando a construção de possíveis atributos ou comportamentos de uma pessoa (Patz; Piaia, 2021).

No processo de tratamento de dados pessoais, o perfilamento de comportamento possibilita uma análise dos padrões de comportamento e das características das pessoas, principalmente, por meio do uso de algoritmos, podendo revelar padrões de consumo, gostos, hábitos e preferências.

Segundo o Idec (2018), por meio da realização de um estudo sobre o uso de aplicativos em consultas médicas, foi possível constatar que esse tipo de análise na área da saúde possibilita o compartilhamento de informações sobre dados médicos para terceiros, o que alimenta a monetização de dados pessoais para o direcionamento de propagandas personalizadas, constituindo, assim, um modelo de negócio.

No estudo de Harayama (2020), identificou-se que os algoritmos têm sido utilizados como uma forma de controlar comportamentos sociais, interferir nas bolsas de valores, nas eleições e na forma de estratificar as redes de socialização. Assim, com o auxílio da Inteligência Artificial (IA) e da medição estatística, são coletados dados dos usuários sobre aspectos de suas vidas que serão utilizados para a elaboração de um quadro de tendências e predição de suas futuras decisões e comportamentos. Essa análise pode acentuar as desigualdades existentes, já que os algoritmos, apesar de serem resultado da IA, refletem os ideais e as visões de mundo dos seres humanos que os programam. E, em muitos casos, a tomada de decisão automática pode refletir vieses discriminatórios, reforçando preconceitos enraizados em nossa sociedade.

Colussi e Santos (2018) apresentaram em seu estudo os possíveis interesses em informações relacionadas ao perfilamento de dados genéticos, que não apenas identificam o sujeito, mas, também, possibilitam traçar um histórico detalhado com as suas características atuais e até futuras, bem como as dos seus familiares, delimitando, assim, a sua herança genética. E essa informação pode, porventura, ser de especial relevância não apenas ao indivíduo submetido ao teste genético – diretamente interessado, aliás –, mas, também aos terceiros, como outras pessoas da família, empregadores, seguradoras, o próprio Estado, entre outros.

Souza, Volles e Ribeiro (2020) mencionaram o perfilamento dos pacientes com diagnóstico da covid-19, realizado durante a pandemia, e afirmam que pode ser tentador o acesso desmedido às informações presentes nos prontuários médicos

dos pacientes sob a justificativa de que a atitude estaria fundada no interesse público de combate ao vírus, alertando que a disponibilização desses dados a terceiros coloca em risco a privacidade dos milhares de indivíduos atendidos pelos sistemas de saúde público e privado.

De acordo com Oliveira (2021), estamos vivenciando a transformação da sociedade da informação para a sociedade da vigilância, na qual as pessoas são monitoradas a fim de regular ou governar o seu comportamento. E isso acontece por meio de uma coleta sistemática dos seus dados pessoais e pela análise desses dados com o intuito de tomar decisões, minimizar riscos, classificar grupos sociais e exercer poder.

Nesse caso, conforme exposto por Harayama (2020) e Rodotà (2008), observamos o uso político das informações para diversos fins e a ideia de vigilância se apresenta como uma característica das relações de mercado, cujo interesse é cada vez mais dispor livremente de um conjunto crescente de informações.

3.3 Privacidade, confidencialidade e segurança da informação

Os estudos analisados trouxeram questões relevantes à privacidade dos dados. Camara *et al.* (2021) afirmam que o compartilhamento de dados pessoais com os provedores de diferentes serviços representa um risco real à privacidade contemporânea. Isso ocorre devido a problemas corriqueiros, como o tratamento inadequado dos dados, a falta de conhecimento dos usuários sobre como seus dados estão sendo compartilhados, o compartilhamento incorreto e o excesso de dados que os próprios usuários finais expõem inadvertidamente.

Em relação à confidencialidade, a abordagem identificada nos estudos se refere à relação médico-paciente. Colussi e Santos (2018) referem que as tecnologias utilizadas nas práticas de telemedicina, telessaúde e *e-Health* podem gerar riscos à confidencialidade inerente à relação médico-paciente, na medida em que há uma exposição das informações passadas pelo paciente e uma insegurança quanto ao armazenamento delas, uma vez que o atendimento é prestado por meio do uso de computadores e conexão via internet.

Quanto à segurança da informação, Coelho e Chioro (2020) problematizam o armazenamento dos dados clínicos dos usuários e a sua centralização em uma única base de dados, o que poderia facilitar, em tese, a organização de ataques cibernéticos visando ao roubo de informação ou mesmo causar instabilidades de repercussão nacional.

A segurança da informação deve ser fundamentada por meio dos pilares de confidencialidade, integridade, disponibilidade e autenticidade do sistema a ser utilizado, o que requer: controles criptográficos; controle de acesso; controle de segurança em rede, proteção física e do ambiente; cópia de segurança; desenvolvimento seguro; gestão de capacidade, gestão de mudanças e gestão de riscos; registros de eventos, rastreabilidade e salvaguarda de *logs*; resposta a incidentes; e segurança *web* (Brasil, 2020).

Considerando o exposto, todos os estudos destacaram a importância de se garantir a privacidade, a confidencialidade e a segurança da informação no processo de coleta e tratamento dos dados dos usuários. Em contrapartida, os estudos também evidenciaram os riscos e as vulnerabilidades existentes que demandam avanços e adequações, de modo a assegurar a proteção de dados pessoais, enquanto um direito.

3.4 Participação dos usuários nas discussões e acesso às informações sobre proteção de dados pessoais

Apenas 27,7% dos estudos analisados trouxeram informações sobre os usuários dos sistemas de saúde nos contextos da saúde digital e da proteção de dados pessoais, mas com enfoque no processo saúde-doença e na vigilância sobre os corpos, e não no usuário como participante desse processo.

Nesse sentido, os estudos apresentaram informações sobre o uso das tecnologias digitais no manejo de doenças crônicas, genéticas e da pandemia de covid-19 (Mattos, 2020; Faria; Cordeiro, 2014; Deboni *et al.*, 2021), mas não abordaram as perspectivas dos usuários, ao se apropriar ou não dessas tecnologias destinadas ao seu cuidado em saúde ou sobre a participação deles nas discussões sobre saúde digital e proteção de dados pessoais.

De acordo com Linke (2019), o usuário se encontra em uma situação de vulnerabilidade e assimetria informacional, visto que não tem conhecimento dos possíveis usos de seus dados, quem terá acesso, por quanto tempo, e as possíveis futuras repercussões negativas disso em sua vida.

Segundo Araujo e colaboradores (2016), a assimetria informacional contribui para que os usuários tenham um escasso conhecimento do uso que se faz dos seus dados pessoais e, por isso, muitas vezes não estão em posição de consentir nem de ter o controle desse uso. Nesse contexto, os operadores de mercado têm interesse em explorar todas as possibilidades dos dados recolhidos para as novas

iniciativas comerciais, todavia, os usuários não têm conhecimento das dinâmicas comerciais que utilizam os seus dados pessoais e de quais são os seus direitos.

Santos (2020) sinalizou a importância de a participação social ter acesso à informação em um contexto de assimetria informacional, técnica e econômica, entre o cidadão e o controlador de dados pessoais. Advoga que o cidadão deve ser identificado como um sujeito vulnerável, havendo a necessidade de que as disposições normativas interfiram no fluxo informacional, facilitando a tomada de decisão do usuário, de modo que o responsabilidade do consentimento não fique a cargo apenas do titular dos dados.

Sarlet e Caldeira (2019) enfatizam a importância do consentimento livre e informado, que é, em síntese, uma das principais garantias que norteiam a relação do paciente com os profissionais de saúde. Ressaltam que a construção do processo de consentir implica a utilização de uma comunicação não diretiva e, no momento em que se sobressai o ambiente digital, apontam para a garantia da transparência no que tange à coleta, à finalidade, ao armazenamento, ao tratamento e à transmissão dos dados.

A ausência dos usuários nas discussões sobre a saúde digital e a proteção de dados pessoais e o não acesso à comunicação e à informação sobre essa temática enfraquece a participação social e a efetivação dos direitos políticos e sociais, sobretudo em relação à proteção de dados e à privacidade que ainda é um assunto desconhecido para a maioria da população.

3.5 Qualificação dos agentes de tratamento dos dados

A pesquisa bibliográfica possibilitou identificar os principais agentes envolvidos na prática de coleta e tratamento dos dados pessoais, representados na figura do governo, das instituições, dos profissionais de saúde e dos profissionais da área de tecnologia e informação. Os estudos analisados enfatizaram a importância da qualificação dos agentes de tratamento dos dados em relação a essa prática.

O estudo de Lemes e Lemos (2020) destacou a necessidade de qualificar os agentes envolvidos, de modo a reforçar a compreensão quanto aos desafios éticos impostos pelas inovações tecnológicas, bem como o entendimento sobre o funcionamento das tecnologias empregadas, especialmente por parte dos que não participaram da criação delas – o que pode acarretar vulnerabilidades à proteção da privacidade e dos dados pessoais.

De acordo com Massarelli e Almeida (2019), os agentes de tratamento de dados devem provar que têm *expertise* para a proteção dos dados que estão sendo postos à disposição deles, não se tratando apenas de mera elucubração documental.

Segundo Pereira (2018), o responsável pelo tratamento de dados tem um dever especial de segurança e confidencialidade, cabendo a adoção de medidas técnicas e organizativas para a proteção dos dados contra tratamentos ilícitos, nomeadamente contra a destruição, perda, alteração, difusão ou acessos não autorizados, principalmente quando envolver a transmissão dos dados por rede. Para além dessas questões, o responsável deve também assegurar um nível de segurança adequado, tendo em conta os conhecimentos técnicos disponíveis, os custos de aplicação, os riscos do tratamento e a natureza dos dados.

Sarlet e Caldeira (2019) afirmam que o tratamento de dados sensíveis aumenta a exigência de uma proteção especial alicerçada nos princípios da dignidade da pessoa humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos direitos humanos. E, nesse sentido, os dados pessoais "devem ser objeto de um tratamento leal, para fins específicos, e com o consentimento da pessoa interessada ou outro fundamento legítimo previsto por lei".

Por meio dessa análise foi possível realizar um diagnóstico inicial e identificar que a qualificação dos agentes de tratamento de dados é uma necessidade, principalmente ao observarmos as fragilidades e os desafios presentes nas instituições e nos serviços de saúde no que se refere à cadeia de coleta e de tratamento dos dados, sendo importante o investimento em práticas de educação continuada e permanente, abordando a temática e a sua operacionalização na prática.

Considerações finais

A inovação tecnológica implica vários desafios éticos, morais e políticos, o que demanda a criação de um ecossistema de saúde digital confiável, seguro, democrático e participativo. Ao analisar os riscos e as vulnerabilidades à proteção de dados pessoais e as implicações, na garantia desse direito, o estudo que deu origem a este texto trouxe para o debate as fragilidades identificadas nos serviços de saúde em suas práticas de coleta e tratamento dos dados, além da necessidade de adequações, em conformidade com a LGPD.

No contexto de digitalização dos serviços de saúde, faz-se necessário falar sobre o uso inadequado dos sistemas informatizados e das suas consequências para os indivíduos e as comunidades, evitando, assim, criar falsos alarmismos públicos e assunções ou juízos morais ou políticos não fundamentados. Importa também, ao mesmo tempo, garantir a segurança e a eficácia das aplicações para os seus utilizadores. E, por fim, assegurar a proteção de dados pessoais e a privacidade como direitos dos cidadãos.

Ainda que a promulgação da LGPD tenha sido um avanço, ela não resolveu todas as questões ligadas ao processo de coleta e tratamento dos dados de saúde já que não aborda a regulamentação de uma estrutura sobre como determinadas situações devem ser consideradas, tais como os processos de gestão, as regras de mercado e os padrões tecnológicos, o que incide em muitas dúvidas no manejo dessas situações, aumentando o grau de risco e de vulnerabilidades à proteção de dados.

Contudo, o reconhecimento no âmbito legal evidencia a importância do direito à proteção de dados pessoais, de modo a promover a dignidade humana e proteger os cidadãos, principalmente em um cenário de mercantilização dos dados pessoais e da saúde.

Referências

ARAGÃO, Suéllyn Mattos de; SCHIOCCHET, Taysa. Lei Geral de Proteção de Dados: desafio do Sistema Único de Saúde. **RECIIS: Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, v. 14, n. 3, p. 692-708, jul.-set. 2020. DOI: https://doi.org/10.29397/reciis.v14i3.2012. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/2012. Acesso em: 8 mar. 2022.

ARAUJO, Alexandra R. *et al.* Saúde móvel: desafios globais à proteção de dados pessoais sob a perspectiva do direito da União Europeia. **RECIIS: Revista Eletrônica de Comunicação, Informação & Inovação em Saúde**, v. 10, n. 4, 12 p. out.-dez. 2016. DOI: https://doi.org/10.29397/reciis.v10i4.1125. Disponível em: https://www.reciis.icict.fiocruz.br/index.php/reciis/article/view/1125. Acesso em: 8 mar. 2022.

BORGES, Wilson Couto; GOMBERG, Estélio; BORGES, Vânia Coutinho Q. Piraí Digital: pioneirismo brasileiro. *In*: NETO, André Pereira; FLYNN, Matthew B. (Eds.). **The Internet and Health in Brazil**: Challenges and Trends. Suíça: Springer Nature, 2019. p. 47-64.

BRASIL. Fiocruz. Comunicação e informação. **Pense SUS**. Disponível em: https://pensesus.fiocruz.br/comunicacao-e-informacao. Acesso em: 8 mar. 2022.

BRASIL. Ministério da Economia. **Guia de avaliação de riscos de segurança e privacidade**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Ministério da Economia, 2020.

BRASIL. Ministério da Saúde. Comitê Gestor da Estratégia e-Saúde. Estratégia e-Saúde para o Brasil. Brasília, DF: MS, 2017. Disponível em: https://www.conasems.org.br/wp-content/uploads/2019/02/Estrategia-e-saude-para-o-Brasil.pdf. Acesso em: 8 mar. 2022.

BRASIL. Presidência da República. **Emenda constitucional n. 115, de 10 de fevereiro de 2022**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 8 mar. 2022.
BRASIL. Presidência da República. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 8 mar. 2022.

BRASIL. Senado Federal. Proposta de emenda à Constituição n. 17, de 2019. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 10 abr. 2022.

CAMARA, Maria Amália Arruda *et al.* Internet das Coisas e blockchain no Sistema Único de Saúde: a proteção dos dados sensíveis diante da Lei Geral de Proteção de Dados. **Cadernos Ibero-Americanos de Direito Sanitário**, Brasília, v. 10, n. 1, p. 93-112, 2021. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/657. Acesso em: 10 abr. 2022.

CARVALHO, Antônio Ramalho de Souza. Os dados no contexto da quarta revolução industrial. *In*: **Proteção de dados pessoais**: privacidade *versus* avanço tecnológico. Cadernos Adenauer XX, n. 3, p. 93-112. Rio de Janeiro: Fundação Konrad Adenauer, out. 2019. Disponível em: https://www.kas.de/documents/265553/265602/Caderno+Adenauer+3+Schutz+von+pers%C3%B6nlichen+Daten.pdf/476709fc-b7dc-8430-12f1-ba21564cde06?version=1.0&t=1571685012573. Acesso em: 10 abr. 2022.

CARVALHO, Victor Miguel Barros de. **O direito fundamental à privacidade ante a monetização de dados pessoais na internet**: apontamentos legais para uma perspectiva regulatória. Dissertação. Mestrado em Direito. Centro de Ciências Sociais Aplicadas. Universidade Federal do Rio Grande do Norte, Natal, 2018. 145 f. Disponível em: https://repositorio.ufrn.br/handle/123456789/26851. Acesso: 10 ab. 2022.

CASTELLS, Manuel. **A sociedade em rede**. 2. ed. São Paulo: Paz e Terra, 1999.

COELHO NETO, Giliate Cardoso; CHIORO, Arthur. Fragmentação e integração entre Sistemas de Informação em Saúde no Sistema Único de Saúde. *In*: CUNHA, Francisco José Aragão Pedroza; BARROS, Susane Santos; PEREIRA, Hernane Borges de Barros. (Orgs). **Conhecimento, inovação e comunicação em serviços de saúde**: governança e tecnologias. Salvador: EDUFBA, 2020. p. 49-68. Disponível em: https://repositorio.ufba.br/bitstream/ri/32104/1/CIC-saude-governanca-miolo-ri.pdf. Acesso em: 10 abr. 2022.

COLUSSI, Fernando Augusto Melo; SANTOS, Tomlyta Luz Velasquez. Novas tecnologias e liberdade de expressão na pesquisa científica: uma análise sobre a proteção de dados genéticos e de saúde. **Revista de Biodireito e Direito dos**

Animais, Porto Alegre, v. 4, n. 2, p. 1- 21, jul.-dez. 2018. Disponível em: https://indexlaw.org/index.php/revistarbda/article/view/4690/pdf. Acesso em: 10 abr. 2022.

DEBONI, Luciane M. *et al.* Desenvolvimento e implementação do atendimento a distância para acompanhamento de pacientes em diálise peritoneal e transplantados renais durante a pandemia de covid-19. **Brazilian Journal of Nephrology**, v. 43, n. 3, p. 422-428, 2021. DOI: 10.1590/2175-8239-JBN-2020-0137. Disponível em: https://www.bjnephrology.org/article/desenvolvimento-e-implementacao-do-atendimento-a-distancia-paraacompanhamento-de-pacientes-em-dialise-peritoneal-e-tranplantados-renais-durantea-pandemia-de-covid-19/. Acesso em: 10 abr. 2022.

DONEDA, Danilo; ALMEIDA, Bethânia de A.; BARRETO, Maurício Lima. Uso e proteção de dados pessoais na pesquisa científica. **Revista Direito Público**, v. 16, n. 90, p. 179-194, nov.-dez. 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3895/Doneda%3B%20Barreto%3B%20Almeida%2C%202019. Acesso em: 10 abr. 2022.

FARIA, Paula Lobato de; CORDEIRO, João Valente. Health data privacy and confidentiality rights: crisis or redemption? **Revista Portuguesa de Saúde Pública**, v. 32, n. 2, p. 123-133, jul. 2014. Disponível em: https://run.unl.pt/bitstream/10362/19858/1/RUN%20-%20RPSP%20-%202014%20-%20v32n2a01%20-%20p.123-133.pdf. Acesso em: 10 abr. 2022.

GOLDIM, José Roberto. **Bioética complexa**: 27 anos na internet 1997-2024. Porto Alegra: UFRGS, 2024.Disponível em: https://www.ufrgs.br/bioetica/. Acesso em: 10 abr. 2022.

HARAYAMA, R. M. Reflexões sobre o uso do Big Data em modelos preditivos de vigilância epidemiológica no Brasil. **Cadernos Ibero-Americanos de Direito Sanitário**, Brasília, set. 2020, v. 9, n. 3, p. 153-165. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/702. Acesso em: 10 abr. 2022.

ICICT; FIOCRUZ; IDEC; INTERVOZES. **Resumo executivo. Proteção de Dados Pessoais em Serviços de Saúde Digital**. Rio de Janeiro: Icict/Fiocruz, out. 2022. Disponível em: https://www.icict.fiocruz.br/sites/www.icict.fiocruz.br/files/resumo_executivo_protecao_de_dados_pessoais.pdf. Acesso em: 10 abr. 2022.

IDEC. **Aplicativos para consultas médicas e direitos dos consumidores**: uma análise qualitativa. São Paulo: Idec, 2018. Disponível em: https://idec.org.br/sites/default/files/arquivos/idec._relatorio_final._aplicativos_de_consultas_medicas._2018.pdf. Acesso em: 10 abr. 2022.

LEMES, M. M.; LEMOS, A. N. L. P. O uso da Inteligência Artificial na saúde pela administração pública brasileira. **Cadernos Ibero-Americanos de Direito Sanitário**, Brasília, v. 9, n. 3, set., 2020, p. 166-182. Acesso em: 10 abr. 2022.

LINKE, Sarah Helena. **Sociedade de vigilância e consumo**: proteção de dados pessoais relacionados à saúde em programas de fidelização de redes de farmácia. Dissertação. Mestrado em Direito. Programa de Pós-graduação em Direito da Universidade Federal de Santa Catarina: Santa Catarina, 2019. 252 f. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/211611/PDPC1443-D.pdf?sequence=-1&isAllowed=y. Acesso em: 10 abr. 2022.

LUPTON, Deborah. **Digital health**: Critical and cross-disciplinary perspectives. Londres: Routledge, 2017.

MASSARELLI JR. José Carlos; ALMEIDA, Verônica Scriptore Freire e. Proteção de dados pessoais como direito fundamental na área da saúde e suas implicações para os profissionais médicos no Brasil cotejando aspectos do direito comparado na União Europeia e na China. **Anais do Encontro Nacional de Pós-Graduação**, v. 3, n. 1, 2019, Universidade Santa Cecília (UNISANTA), Santos. Disponível em: https://ojs.unisanta.br/index.php/ENPG/article/view/2193/1691. Acesso em: 10 abr. 2022.

MATTOS, Alexandre Magalhães de. **Doença crônica Brasil**: aplicativo para os direitos aos portadores de agravos crônicos à saúde. Dissertação. Mestrado Profissional. Programa de Pós-Graduação em Saúde e Tecnologia no Espaço Hospitalar/ PPGSTEH. Universidade Federal do Estado do Rio de Janeiro/UniRio, 2020. 112 f. Disponível em: http://www.repositorio-bc.unirio.br:8080/xmlui/bitstream/handle/unirio/13142/Relatorio%20da%20pesquisa%20Alexandre%20Mattos.pdf?sequence=1&isAllowed=y. Acesso em: 10 abr. 2022.

OLIVEIRA, Samuel R. de. **Sorria, você está sendo filmado!**: repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters, Revista dos Tribunais, 2021.

ONU. Pandemia de covid-19 expôs desigualdade digital em todo o mundo. **Onu News**, 2020. Disponível em: https://news.un.org/pt/story/2020/07/1720021. Acesso em: 10 abr. 2022.

OPAS. OMS divulga primeira diretriz sobre intervenções de saúde digital, abr. 2019. Disponível em: https://www.paho.org/pt/noticias/17-4-2019-oms-divulga-primeira-diretriz-sobre-intervencoes-saude-digital. Acesso em: 10 abr. 2022.

PATZ, Stéfani Reimann; PIAIA, Thami Covatti. Vigilância, perfilamento e tratamento de dados pessoais no contexto do controle migratório. **RDP**, Brasília, v. 18, n. 100,

p. 690-720, out./dez. 2021. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5999/pdf. Acesso em: 10 abr. 2022.

PEREIRA, Alexandre L. Dias. Big Data, e-Health e Autodeterminação Informativa: A Lei 67/98, a Jurisprudência e o Regulamento 2016/679. Lex Medicinae - Revista Portuguesa de Direito da Saúde, n° 29, 2018. Disponível em: https://estudogeral.uc.pt/bitstream/10316/48094/1/Big%20data%20ehealth%20autodeterminacao%20informativa.pdf. Acesso em: 10 abr. 2022.

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

QUINTILIANO, Leonardo David. A proteção de dados pessoais e as competências dos entes federativos – Análise dos efeitos da PEC 17/2019. **Migalhas**, n. 5.915, 26 nov. 2021. Disponível em: https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/355602/a-protecao-de-dados-pessoais-e-as-competencias-dos-entes-federativos. Acesso em: 10 abr. 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

SALIM, Leila. Seus dados valem ouro: vazamentos de dados pessoais de saúde reforçam urgência do debate sobre privacidade, proteção de informações sensíveis e direitos no ambiente digital. **Escola Politécnica de Saúde Joaquim Venâncio**. EPSJV; Fiocruz, 7 jun. 2021. Disponível em: https://www.epsjv.fiocruz.br/noticias/reportagem/seus-dados-valem-ouro. Acesso em: 10 abr. 2022.

SANTOS, Samanda Pereira. **A eficácia dos direitos fundamentais na sociedade da informação**: uma análise acerca da proteção e promoção de dados em matéria de saúde. Trabalho de conclusão de curso. São Luís: Centro Universitário UNDB, 2020. Disponível em: http://repositorio.undb.edu.br/handle/areas/442. Acesso em: 10 abr. 2022.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. 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, p. 1-27, 2019. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/411. Acesso em: 10 abr. 2022.

SARLET, Ingo Wolfgang; KEINERT, Tania Margarete Mezzomo. O direito fundamental à privacidade e as informações em saúde: alguns desafios. *In*: KEINERT, T. M. M.; SARTI, F. M.; CORTIZO, C. T.; PAULA, S. H. B. de. (Orgs.). **Proteção à privacidade**

e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015. p. 113-145. Temas em Saúde Coletiva 18. Disponível em: https://portolivre.fiocruz.br/prote%C3%A7%C3%A3o-%C3%A0-privacidade-e-acesso-%C3%A0s-informa%C3%A7%C3%B5es-em-sa%C3%BAde-tecnologias-direitos-e-%C3%A9tica. Acesso em: 10 abr. 2022.

SILVA, Iza Sherolize Américo da; MARQUES, Isaac Rosa. Conhecimento e barreiras na utilização dos recursos da Tecnologia da Informação e Comunicação por docentes de enfermagem. **Journal of Health Informatics**, v. 3, n. 1, jan.-mar. 2011, p. 3-8. Disponível em: https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/127. Acesso em: 10 abr. 2022.

SOUZA, Joyce Aryane. **A saúde dos dados pessoais e o município de** São Caetano do Sul. Dissertação de Mestrado em Ciências Humanas e Sociais. Universidade Federal do ABC – UFABC, São Paulo, 2018. 142 f.

SOUZA, Leonardo da Rocha de; VOLLES, Guilherme Augusto; RIBEIRO, Marcelo. O prontuário do paciente na área médica: direito ao sigilo *versus* interesse público sanitário na pandemia da covid-19. **Revista Pensamento Jurídico**, São Paulo, v. 14, n. 2, edição especial "Covid-19". 2020, p. 388-409. Disponível em: https://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/RPensam-Jur_v.14_n.2.18.pdf. Acesso em: 10 abr. 2022.

STEVANIM, Luiz Felipe; MURTINHO, Rodrigo. **Direito à comunicação e saúde**. Rio de Janeiro: Editora Fiocruz, 2021.

https://doi.org/10.29397/EdicoesLivres/20250112

A proteção de dados pessoais em serviços de saúde digital: apontamentos sobre documentos nacionais e padrões internacionais

Juliana Ruiz
Maria Luciano
Paulo Victor Melo

Como órgãos de governo em âmbito federal e conselhos profissionais de saúde têm formulado e operacionalizado regulações a respeito do uso de dados pessoais no setor? É possível identificar padrões internacionais de proteção de dados em saúde que possibilitem usos mais criativos do direito e novas formas de pensar questões jurídicas sobre o tema na realidade brasileira? A busca por pistas para responder a essas duas questões motivou, no âmbito do projeto Proteção de Dados Pessoais em Serviços de Saúde Digital, a realização de uma revisão documental em legislações nacionais e de outros países.

Aceleradas pelo contexto da pandemia de covid-19, as iniciativas de saúde digital representam uma tendência na ação de diferentes governos, em geral relacionadas à necessidade de eficiência dos serviços e a uma concepção de irreversibilidade do uso das tecnologias digitais. Assim, expressões como "telemedicina", "*e-health*", "teleconsulta", entre outras, passaram a compor o repertório tanto de gestores públicos quanto de profissionais das diferentes especialidades da saúde.

Um dos aspectos relevantes nesse contexto, e de particular interesse da pesquisa em que este capítulo se insere, diz respeito aos dados dos usuários e usuárias. Souza (2018) alerta, por exemplo, para a necessidade de análises que evidenciem os compartilhamentos de dados entre os setores público e privado, a transparência na gestão, o tratamento das informações e o cumprimento das determinações legais relativas à proteção dos dados pessoais.

Visando contribuir com a reflexão sobre os impactos dos usos e do tratamento de dados pessoais nos serviços de saúde digital, uma das ações da pesquisa foi a revisão e a análise documental de legislações brasileiras e de outros países que apontem o entrecruzamento entre proteção de dados e saúde digital. Este capítulo apresenta a metodologia da revisão documental e a análise desses documentos normativos e legais, tendo a proteção dos dados pessoais dos usuários e usuárias como objetivo.

Metodologia

Em nível nacional, a pesquisa realizou investigação em bases de dados de órgãos do Governo Federal e de conselhos federais da área de saúde[1], sendo a definição dessas instituições a partir da identificação de segmentos diretamente envolvidos nas questões de saúde digital e tomando em consideração a complexidade do modelo regulatório brasileiro na área de saúde (Aith; Germani; Balbinot; Dallari, 2018), que prevê atribuições para ministérios, Conselho Nacional de Saúde, câmaras temáticas e mesas de negociação, além de conselhos de 14 categorias profissionais.

Já em relação aos padrões internacionais, compreendeu-se ser fundamental a análise de como os principais órgãos multilaterais e regionais na área da saúde têm definido mecanismos regulatórios e adotado práticas positivas no uso de dados em saúde. Assim, justifica-se a articulação pela pesquisa de normativas a respeito do tema emanadas por instituições como a Organização Mundial da Saúde (OMS), agência especializada das Nações Unidas destinada às questões relativas à saúde; a Organização Pan-Americana da Saúde (OPAS), agência internacional especializada em saúde das Américas e organização internacional de saúde pública mais antiga do mundo; e o Africa Centres for Disease Control and Prevention (Africa CDC), agência de saúde pública da União Africana. Essa seleção se deu a partir da constatação de que a análise do sistema jurídico perpassa o contexto em que se insere o problema jurídico verificado, compreendendo os debates teóricos e o modelo regulatório adotado, bem como as questões políticas, sociais e econômicas. Buscou-se, assim, investigar a produção normativa de instituições representativas de realidades distintas.

De igual modo, demonstrou-se relevante investigar como o European Data Protection Board (EDPB), organismo europeu independente que contribui para a aplicação de regras em matéria de proteção de dados na União Europeia, tem dedicado atenção ao uso de dados na saúde. Afinal, esse órgão tem liderado os debates a respeito da aplicação e regulamentação da General Data Protection Regulation (GDPR), marco regulatório europeu no campo de proteção de dados pessoais que tem inspirado legislações pelo mundo, entre as quais a Lei Geral de Proteção de Dados Pessoais (LGPD – lei n. 13.709/2018).

Outra estratégia pertinente, não ignorando as diferenças entre as realidades de cada local, foi observar como alguns países com uma cultura de proteção de dados pessoais lidam com essa temática na área da saúde. Nesse sentido, foram escolhidos o Information Commissioner's Office (ICO) e a Commission Nationale de l'Informatique et

1 Rede de Informação Legislativa e Jurídica (LexML); Agência Nacional de Saúde (ANS); Agência Nacional de Vigilância Sanitária (Anvisa); Conselho Nacional de Saúde (CNS); Conselho Federal de Medicina (CFM); Conselho Federal de Enfermagem (Cofen); Conselho Federal de Farmácia (CFF); Conselho Federal de Biomedicina (CFBM).

des Libertés (CNIL), órgãos respectivamente do Reino Unido e da França que se afirmam pela defesa dos direitos de informação e preservação das liberdades individuais.

Importante enfatizar que tal estratégia metodológica partiu da compreensão de que a comparação, ao invés de permitir a mera reprodução de institutos estrangeiros, pode permitir usos mais criativos do direito e das novas formas de pensar questões jurídicas a respeito da realidade local que de outra forma seriam ignoradas ou subanalisadas (Veçoso, 2019).

Selecionados os órgãos nacionais e internacionais a investigar, encaminhou-se a definição dos descritores de busca, estratégia adequada em pesquisas com bases de dados diversas (Neves; Maciel, 2019) e, mais especificamente, na área da informação em saúde.

Desse modo, e considerando que a definição de termos amplos não fornecia resultados relevantes, optou-se inicialmente por descritores mais direcionados, utilizando, em alguns casos, a combinação de descritores. Assim, os descritores empregados nas bases de dados brasileiras foram: "acesso e proteção de dados pessoais", "dados sensíveis e dado sensível", "direito à comunicação", "direito à saúde", "informação em saúde", "inovação em saúde", "proteção de dados", "risco em saúde", "saúde digital", "sistemas de informação", "telemedicina", "telessaúde", "tratamento de dados sensíveis", "uso de dados de saúde", "LGPD". Já para os documentos internacionais foram aplicados os seguintes descritores: "*e-health*", "*mobile health*", "*telemedicine*", "*digital health*", "*telehealth*", "*data protection*".

Uma dificuldade metodológica em relação aos descritores foi o fato de muitos *sites* não permitirem a inserção de termos, mas já disponibilizarem previamente um conjunto de "temas".[2]

A partir desses descritores e dentro das possibilidades apresentadas nas bases de dados mencionadas anteriormente, foram identificados, inicialmente, 1.036 documentos, sendo 703 de legislação federal, 218 de órgãos internacionais e 115 de conselhos profissionais e agências reguladoras nacionais.

De forma a garantir uma análise mais detalhada em relação aos objetivos da pesquisa, foram excluídos, no processo de mineração e análise, todos os resultados que não tratavam de proteção de dados pessoais nem de regulação em saúde, além de decisões judiciais e notícias (no caso dos *sites* internacionais), totalizando-se, ao

2 Este foi o caso, por exemplo, do CFM e da OPAS. No CFM, buscou-se as documentações a partir dos seguintes temas: tecnologia da informação em saúde; tecnologia em saúde; tecnologia em medicina; telemedicina. Já na OPAS, o caminho adotado foi realizar a pesquisa em dez "temas": Atenção Primária à Saúde (APS); *risk and outbreak communication*; conhecimento e inovação em saúde; *cultural diversity and health*; equidade de gênero em saúde; *medicines and health technologies*; *environmental determinants of health*; *health equity*; *health technology assessment*; *integrated health services network*.

final, 88 documentos, sendo 60 de âmbito nacional (Brasil) e outros 28 internacionais (regionais e de outros países).

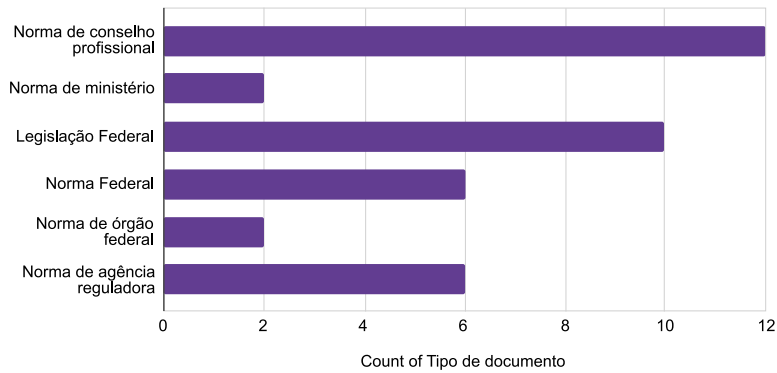
Para um maior rigor da análise, em um primeiro momento, decidiu-se focar nos documentos encontrados na esfera nacional. Após leitura da legislação levantada, selecionou-se um total de 38 documentos, que baseiam a análise aqui apresentada.

Definido o *corpus*, a etapa seguinte envolveu a elaboração de um roteiro de análise, a partir de um formulário que permitisse a inserção, pela equipe de pesquisa, do máximo de informações sobre cada documento. Esse formulário foi estruturado em sete seções, com um conjunto de perguntas cada, além de dois campos: um para identificação do(a) pesquisador(a) e outro para comentários gerais.

Principais resultados

Adotados os procedimentos metodológicos anteriormente descritos, o primeiro resultado a considerar, conforme demonstrado no Gráfico 1, diz respeito ao fato de os documentos nacionais serem majoritariamente normas de conselhos profissionais (boa parte emitida pelo CFM) e de legislação federal. Quando se fala em "normas federais", pode-se referir a decretos presidenciais, normas emitidas pelo Legislativo (decreto legislativo), entre outros tipos de normativas que não podem ser classificadas como leis federais. Na categoria "norma de órgão federal", foi possível encontrar duas normas da Receita Federal do Brasil.

Gráfico 1 – Tipos de documento



Fonte: Elaborado pelos autores (2024).

Sobre o ano do documento, como pode ser visto na Tabela 1, a maioria foi editada/elaborada a partir de 2017 e, mais ainda, a partir de 2018, após as promulgações do

Marco Civil da Internet (MCI ou lei n. 12.965/2014) e da Lei Geral de Proteção de Dados Pessoais (LGPD ou lei n. 13.709/2018, com entrada em vigor em setembro de 2020), confirmando a nossa hipótese inicial de ter havido uma maior formulação legislativa e normativa sobre proteção de dados pessoais, a partir de legislações federais orientadoras.

No entanto, conforme será indicado na análise do conteúdo das normas, mesmo aquelas que são posteriores à LGPD ou ao MCI acabam não trazendo, em detalhes, instruções de como devem ser as operações envolvendo o tratamento de dados pessoais, entre outras medidas.

Tabela 1 – Anos dos documentos

Anos	Número de normas
2021	3
2020	11
2019	2
2018	3
2017	4
2016	2
2015	3
2014	3
2012	3
2007	1
2002	1
2001	1
2000	1

Fonte: Elaborada pelos autores (2024).

Outro resultado a destacar é que, dos documentos publicados a partir de 2020, apenas sete mencionam explicitamente os conceitos de "dado pessoal" ou "dado pessoal sensível" e apenas seis mencionam explicitamente a LGPD. No entanto, a maioria dessas menções não traz informações adicionais e específicas em relação a como a LGPD deverá ser implementada, e, sim, enuncia-se que a LGPD deverá ser observada, sem oferecer maior detalhamento. Por exemplo, na portaria 1.434/2020, indica-se que as diretrizes da LGPD e da lei n. 12.527/2011 (Lei de Acesso à Informação ou LAI) devem ser seguidas, sem oferecer maiores detalhes de como isso deverá ser feito.

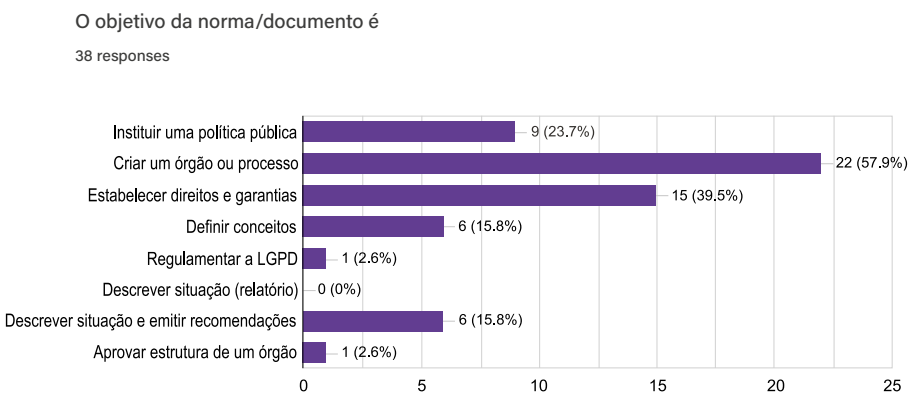
Isso pode representar um problema, visto que apesar de a LGPD ser uma legislação bastante extensa e se aplicar para tratamentos de dados pessoais nos setores

público e privado (LGPD, art. 3º, *caput*), há ainda muitos pontos a serem discutidos e regulamentados, especialmente no que diz respeito a dados sensíveis e operações de saúde.

Uma exceção é a resolução n. 649/2020 do Conselho Federal de Enfermagem (Cofen), a qual versa sobre a possibilidade de fornecimento de dados de profissionais de enfermagem pelo Cofen. Nela, há a menção de que a LGPD deve ser considerada na aplicação da legislação e até mesmo a reprodução quase integral de alguns artigos da LGPD.[3] Essa resolução ainda estabelece algumas balizas e alguns critérios para o compartilhamento de dados pessoais de profissionais de enfermagem pelo Cofen.

Outro resultado da análise é o fato de a maioria dos documentos e das normas analisados ter como objetivos, como pode ser verificado no Gráfico 2, o estabelecimento de direitos e garantias, a criação de um órgão ou procedimento e a descrição de situações com emissão de recomendações – pontos que estão em sintonia com o caráter recente das legislações orientadoras citadas acima, mais precisamente o MCI e a LGPD.

Gráfico 2 – Objetivos dos documentos/normas

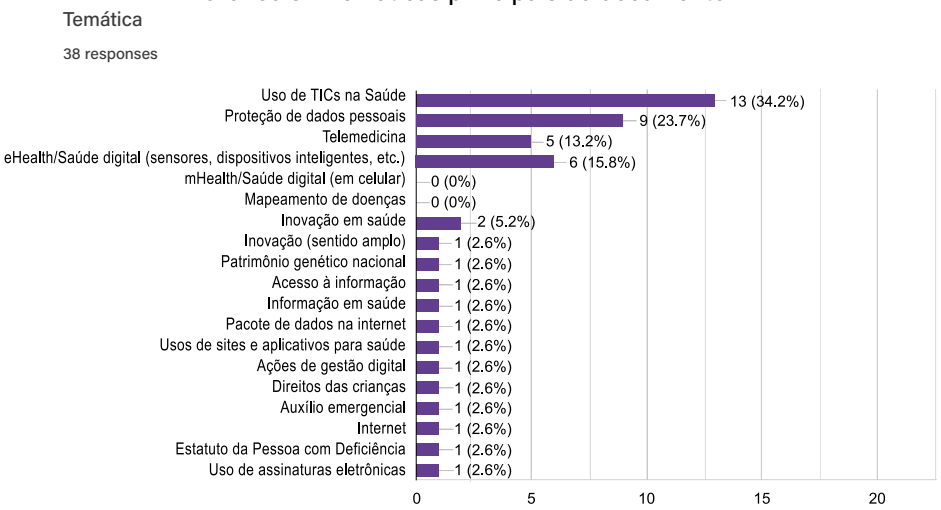


Fonte: Elaborado pelos autores (2024).

3 Diz a resolução do Cofen: "Art. 3º O fornecimento de dados pessoais às Pessoas Jurídicas de Direito Público somente poderá ser realizado nas seguintes hipóteses: I – para o cumprimento de obrigação legal ou regulatória pelo Cofen; II – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; III – para a realização de estudos por órgão de pesquisa, em especial da saúde pública, garantida, sempre que possível, a anonimização dos dados pessoais; IV – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; V – para a proteção da vida ou da incolumidade física do titular ou de terceiro; VI – para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; VII – quando necessário para atender aos interesses legítimos e que trouxerem benefícios ao Sistema Cofen/Conselhos Regionais de Enfermagem, ou à categoria de enfermagem, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais" (Resolução n. 649/2020 do Cofen).

Em relação aos temas, nos documentos e nas normas observou-se, como pode ser verificado no Gráfico 3, que os principais temas foram: "Saúde", "Uso de TICs na saúde", "Proteção de dados pessoais", "Telemedicina"; e "*e-Health*/Saúde digital", com muitos documentos tratando de dois ou mais assuntos.

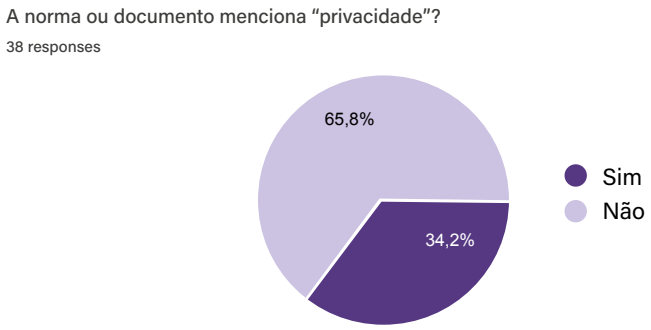
Gráfico 3 – Temáticas principais do documento

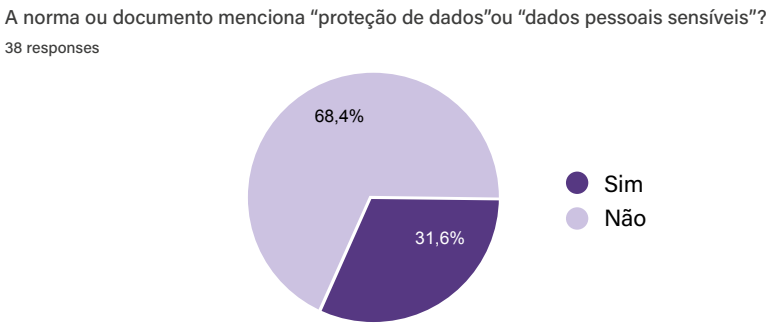


Fonte: Elaborado pelos autores (2024).

Ainda em termos de resultados da análise, apesar de o uso das palavras-chave privilegiar essa questão, pode-se verificar que menos de um terço das legislações estão dentro da temática de proteção de dados pessoais, conforme indicado nos Gráficos 4 e 5.

Gráficos 4 e 5 – Menção à privacidade e aos dados pessoais





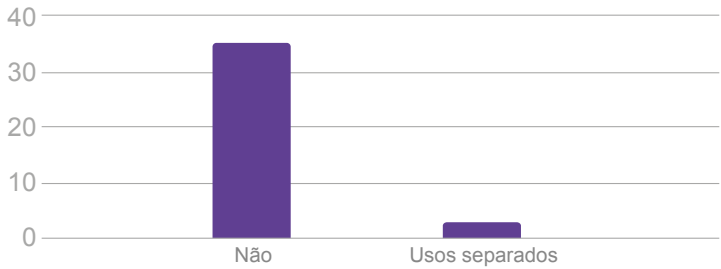
Fonte: Elaborados pelos autores (2024).

Vale enfatizar ainda que, se considerado o conjunto dos documentos analisados, a maioria das normas não menciona nem privacidade nem proteção de dados pessoais. Ao considerarmos apenas os documentos editados a partir de 2018 (19 normas), 12 não mencionam privacidade e sete o fazem; no que se refere à proteção de dados ou dados pessoais sensíveis, nove documentos não mencionam, enquanto dez mencionam. Ou seja, há um aumento considerável da incidência desses termos a partir de 2018.

Apesar disso, a análise mais aprofundada do conteúdo dos documentos indica que ainda há bastante imprecisão conceitual sobre esses temas, com termos que têm significados distintos sendo, em alguns casos, tratados como sinônimos.

A título de exemplo, nenhum dos documentos diferencia de maneira expressa “privacidade” e “proteção de dados pessoais”, conforme pode ser visto no Gráfico 6. Quando muito, há o uso desses termos com conotações diferentes (em três casos, como pode ser visto no gráfico a seguir), mas em nenhum dos casos há preocupação em explicar o que está por trás da diferença entre esses dois conceitos.

Gráfico 6 – Diferenciação entre proteção de dados e privacidade



Fonte: Elaborado pelos autores (2024).

Compreende-se, aqui, que essa imprecisão pouco colabora com o entendimento do conjunto da população sobre as diferenças entre os dois conceitos que, segundo Vergili (2019), vão de aspectos como origem e objeto até previsão no ordenamento jurídico brasileiro, entre outros.

A começar pelo direito à privacidade, este surge com a identificação de um indivíduo titular de direitos oponíveis ao Estado. Trata-se da necessidade de permitir espaço para o desenvolvimento particular do indivíduo e [de] seus pensamentos, sem a imposição da autoridade pública sobre o seu agir e pensar íntimos [...]. O direito à proteção de dados pessoais, por sua vez, origina-se posteriormente ao direito à privacidade. É resultado da sociedade da informação. Com o surgimento de computadores e, em seguida, bancos de dados, o controle sobre a informação – e, em especial, dados pessoais – passa a ser visto como uma forma de poder. A preocupação com a proteção de dados pessoais deriva da percepção da amplitude e potencialidade de controle e manipulação sobre a sociedade e o mercado que este tipo de dado oferece. (Vergili, 2019, s.p.)

Outro apontamento da pesquisa diz respeito ao fato de somente cinco das legislações editadas a partir de 2018 regularem algum ponto específico da LGPD. Ainda assim, ao analisar especificamente o que essas normas regulamentam, indica-se o seguinte: em dois casos há o desenho da Autoridade Nacional de Proteção de Dados (ANPD); em outros dois casos, conselhos profissionais regulamentam situações específicas e utilizam-se da LGPD para estabelecer alguns parâmetros. Por fim, há a portaria GM/MS n. 1.768/2021 que estabelece diversos parâmetros de proteção de dados, no entanto, de ordem genérica, que não preveem medidas específicas para a implementação de proteção de dados.

Tabela 2 – Pontos regulados da LGPD nas legislações analisadas

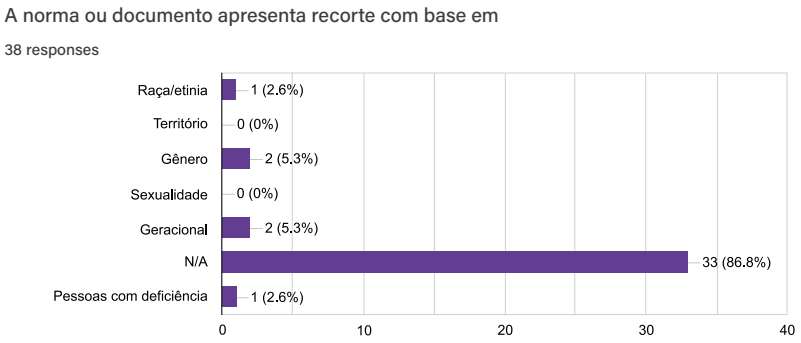
Normas	Pontos da LGPD que a norma regulamenta
Lei n. 13.853/2019	Regulamenta a Autoridade Nacional de Proteção de Dados (ANPD), prevista no artigo 5º da LGPD.
Decreto n. 10.474/2020	Estabelece a Autoridade Nacional de Proteção de Dados (ANPD), prevista no artigo 5º da LGPD.

Resolução Cofen n. 649/2020	A norma libera o compartilhamento de dados de profissionais por parte do Cofen para autoridades públicas competentes (art. 2º), além de liberar para outras funções como: (i) cumprimento de obrigação legal ou regulatória pelo Cofen; (ii) situações em que há a possibilidade de se realizar pesquisas. Ainda, indica-se que o Cofen não será responsável pelo uso indevido de dados por terceiros.
Resolução CFM n. 2.299/2021	Estabelecimento de algumas condições para determinadas transações ocorrerem via documentos eletrônicos.
Portaria GM/MS n. 1.768/2021	Vários artigos estabelecem responsabilidades de proteção de dados. Art. 4º São diretrizes gerais de governança e gestão da Política Nacional de Informação e Informática em Saúde (PNIIS): VIII – estabelecimento de mecanismos de controle de acesso autorizado a dados pessoais e dados pessoais sensíveis, pelo usuário, pelos profissionais de saúde, gestores da atenção e vigilância em saúde, órgãos de pesquisa e agentes públicos legalmente autorizados, em conformidade com a lei n. 13.709, de 14 de agosto de 2018 (Redação dada pela PRT GM/MS n. 1.768 de 30 de julho de 2021).

Fonte: Elaborada pelos autores (2024).

Outro apontamento sobre o conjunto de documentos e normas é a ausência, de um modo geral, de informações mais específicas sobre determinados segmentos populacionais, quais sejam: critérios de raça/cor, território, gênero, geracional e sexualidade são marcadores importantes também, quando os assuntos são saúde digital e proteção de dados pessoais. Das 38 normas analisadas, apenas cinco[4] trazem algum tipo de recorte direcionado a um público específico, de acordo com o Gráfico 7.

Gráfico 7 – "Recortes" apresentados no documento



Fonte: Elaborado pelos autores (2024).

4 O decreto n. 10.488/2020, o qual institui auxílio emergencial residual para o enfrentamento da covid-19, apresenta questões de gênero e geracionais, por isso que a contagem do documento indica seis documentos.

Particularmente num país como o Brasil, caracterizado pela produção de violências estruturais de raça, gênero e sexualidade, a elaboração de documentos normativos, reguladores ou orientadores de políticas públicas não pode prescindir da disponibilização de informações e dados desagregados, questão que é, inclusive, objeto de preocupação por organismos internacionais da área de saúde, a exemplo da OPAS.

Dados desagregados oferecem muitos benefícios, tais como: análise acurada da situação de saúde; melhor entendimento das características específicas de uma população; detecção de problemas; identificação de padrões e necessidades; monitoramento da equidade; estruturas e planos de financiamento para o direcionamento de recursos; monitoramento e avaliação de projetos; avaliação dos avanços; comparações de rotina e análise de tendências para informar e melhorar os programas; melhores sistemas de informação em saúde; entre outros. (OPAS, 2020, p. 2)

A própria LGPD traz algumas previsões no sentido de que dados agregados (desde que esse procedimento tenha sido feito de maneira correta, com pouca possibilidade de identificar uma pessoa natural) não seriam considerados dados pessoais. Nesse sentido, é importante que as instituições saibam aplicar parâmetros de anonimização e agregação de dados de acordo com o contexto no qual estão inseridas como forma de continuar a oferecer informações de interesse público à sociedade.

Como, por exemplo, abordar temas como saúde digital ou telemedicina e não mencionar as desigualdades de acesso à internet e às tecnologias digitais de informação e comunicação? Alguns números da mais recente edição da pesquisa TIC Domicílios[5] ajudam no entendimento do cenário:

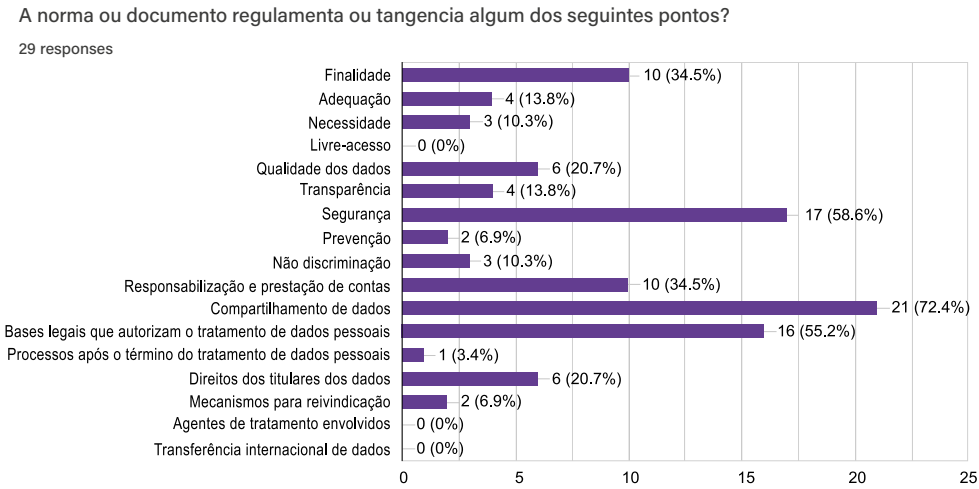
- Apenas 17% dos domicílios na zona rural têm computador. Nas zonas urbanas, 50%.
- Somente 13% das pessoas das classes D e E têm computador em casa. Na classe C, 50%; na classe B, 85%; e na classe A, o índice é de 100%.
- 84% das pessoas que vivem em áreas rurais acessam internet exclusivamente pelo celular. Nas áreas urbanas, 54%.

5 Realizada anualmente desde 2005, pelo Comitê Gestor da Internet no Brasil (CGI.br), a TIC Domicílios tem o objetivo de mapear o acesso às TIC nos domicílios urbanos e rurais do país e as suas formas de uso por indivíduos de 10 anos de idade ou mais. Link para a pesquisa completa: https://cetic.br/pesquisa/domicilios/.

- 90% das pessoas das classes D e E acessam internet exclusivamente pelo celular, percentual consideravelmente inferior às classes C (58%); B (25%); e A (11%).
- 62% das mulheres e 65% das negras e negros usam internet exclusivamente pelo celular (entre os homens, o percentual é de 52%; e entre as pessoas brancas é de 48%).

No que se refere aos pontos essenciais presentes em legislações orientadoras de proteção de dados, estão listados a seguir os assuntos predominantes nos documentos (lembrando que um documento pode mencionar mais de um assunto ao mesmo tempo):

Gráfico 8 – Assuntos contemplados no documento



Fonte: Elaborado pelos autores (2024).

Há três temáticas predominantes: **(i)** indicação de agentes de tratamento envolvidos na atividade; **(ii)** compartilhamento de dados; e **(iii)** indicação de medidas de segurança da informação.

Quanto a (i), muitas das normas indicam quais seriam os agentes de tratamento envolvidos em determinada operação (médicos, enfermeiros, instituições de saúde, entre outros). Como a maioria das normas acaba tangenciando esse assunto,

agentes de tratamento é um dos temas que mais pode ser identificado, apesar de nem sempre eles estarem explicitamente indicados como tal.

Quanto a (ii), algumas normas indicam as circunstâncias nas quais os dados poderão ser compartilhados ou, simplesmente, indicam que dados poderão ser compartilhados.[6] Na maioria dos casos, as previsões são genéricas, afirmando que os agentes deverão adotar medidas relativas à segurança dos dados e à preservação de seu sigilo, quando for o caso.

Por fim, (iii), muitas das normas indicam que os dados devem ser tratados com segurança, mas geralmente apresentam abordagens generalistas e superficiais, sem a definição de medidas técnicas e administrativas. Por um lado, entendemos que é importante que seja dado aos agentes de tratamento certo espaço para que decidam sobre determinadas medidas de segurança, visto que sua efetividade dependerá do contexto na qual estão inseridas e que diferentes agentes e setores terão parâmetros distintos. Por outro, a demasiada generalidade das normas pode fazer com que agentes não saibam quais são as iniciativas necessárias para proteger os dados pessoais sob sua tutela.

Outro ponto a ser destacado é que o "consentimento" aparece de forma recorrente em diversos documentos. No universo analisado, sete citam o consentimento como necessário para a realização de determinadas atividades. Entre eles, estão: (i) o consentimento do paciente ao médico para revelar conteúdos de seu prontuário para terceiros (despacho CFM n. 373/2016, resolução CFM n. 1.643/2002, resolução CFM n. 1.605/2000); (ii) o consentimento do paciente para a transmissão eletrônica de imagens de seus exames para terceiros (resolução CFM n. 2.264/2019, resolução CFM n. 2.107/2014); (iii) o consentimento para o acesso ao conhecimento tradicional associado de origem identificável (lei n. 13.123/2015); e (iv) o consentimento para a pesquisa científica. Nesse sentido, há uma necessidade de releitura dessas normas pelos órgãos competentes como forma de indicar se o significado de "consentimento" empregado originalmente é o mesmo referido pela LGPD, entre outras medidas.

Quanto a (i) e (ii), essas hipóteses poderiam entrar em conflito com a LGPD em alguns pontos. Em primeiro lugar, a LGPD afirma que o consentimento deve ser manifestação livre, informada e inequívoca pela qual o titular concorda com as finalidades para determinada atividade de tratamento (LGPD, art. 5º, XII). Em segundo lugar, o art. 8º, § 5º da LGPD determina que o consentimento

6 O art. 11º, § 4º, da LGPD é especialmente nesse sentido.

pode ser revogado a qualquer momento mediante manifestação expressa do titular e que, eventualmente, esses dados podem ser eliminados. No entanto, com a complexidade das tecnologias aplicadas ao atendimento ao paciente, eventualmente a transmissão eletrônica de determinados dados pode ser a única forma de prestar alguns tipos de serviço, de forma que devemos inquirir se o consentimento seria realmente livre, nesse tipo de situação, e se ele seria a base legal adequada para esse tratamento. Em outras palavras: apesar de outras normas mencionarem "consentimento", esse consentimento seria equivalente ao consentimento como base legal da LGPD?

Chama a atenção, por fim, que apenas três documentos mencionem, autorizem ou definam a criação de algum aplicativo ou *software* específico relacionado à saúde digital. A análise permite afirmar ainda que há, em geral, pouco "diálogo" entre os próprios documentos. Nesse sentido, alguns indicadores demonstram que boa parte do material pesquisado não faz qualquer referência a outras normas de proteção de dados pessoais e, quando o faz, é de forma superficial.

Referências

AITH, F. M. A.; GERMANI, A. C. C.; BALBINOT, R.; DALLARI, S. G. Regulação do exercício de profissões de saúde: fragmentação e complexidade do modelo regulatório brasileiro e desafios para seu aperfeiçoamento. **Revista de Direito Sanitário**, São Paulo, v. 19 n. 2, p. 198-218, jul./out. 2018. Disponível em: https://www.revistas.usp.br/rdisan/article/view/152586. Acesso em: 15 jun. 2024.

NEVES, Henrique John Pereira; MACIEL, Andrea Orengo. A metodologia em uma pesquisa. **JUS.com.br**. 21 jun. 2019. Disponível em: https://jus.com.br/artigos/74862/a-metodologia-em-uma-pesquisa. Acesso em: 15 jun. 2024.

OPAS/PAHO. ORGANIZAÇÃO PAN-AMERICANA DA SAÚDE. **Por que a desagregação de dados é essencial durante pandemias**. Organização Pan-Americana de Saúde, 2020. Disponível em: https://www3.paho.org/ish/images/docs/Data-Disaggregation-Factsheet-Portuguese.pdf?ua=1. Acesso em: 15 jun. 2024.

SOUZA, Joyce Ariane de. **A saúde dos dados pessoais e o município de São Caetano do Sul**. Dissertação de mestrado. Programa de Pós-graduação em Ciências Humanas e Sociais da Universidade Federal do ABC, 2018. Disponível em: https://bdtd.ibict.br/vufind/Record/UFBC_ccbcc3bedad482ccb9952a90e965a20e Acesso em: 15 jun. 2024.

VEÇOSO, Fabia Fernandes Carvalho. Achtung baby! Ou porque meu trabalho acadêmico não precisa de direito comparado... até que se prove o contrário. *In*: QUEIROZ, Rafael Mafei Rabelo; FEFERBAUM, Marina. (Coords.). **Metodologia da pesquisa em direito**: técnicas e abordagens para elaboração de monografias, dissertações e teses. 2. ed. São Paulo: Saraiva, 2019.
VERGILI, Gabriela Machado. Análise comparativa entre direito à privacidade e direito à proteção de dados pessoais e relação com o regime de dados públicos previsto na Lei Geral de Proteção de Dados. **DataPrivacyBR**. 18 set. 2019. Disponível em: https://dataprivacy.com.br/analise-comparativa-entre-direito-a-privacidade-e-direito-a-protecao-de-dados-pessoais-e-relacao-com-o-regime-de-dados-publicos-previsto-na-lei-geral-de-protecao-de-dados-2/. Acesso em: 15 jun. 2024.

AUTORES

Angélica Baptista Silva

Especialista em Internet, interface e multimídia e com PhD em Saúde Pública. Pesquisadora da Fundação Oswaldo Cruz, professora visitante na Universidade de Aveiro (2023-2024) e do quadro permanente da Pós-graduação Stricto sensu em Ensino em Biociências e Saúde do Instituto Oswaldo Cruz. Coordena o curso Direitos Humanos, Gênero e Sexualidade da ENSP, o Laboratório Setorial Saúde Coletiva / Atenção Primária / Humanidades da Plataforma Internacional para Ciência, Tecnologia e Inovação em Saúde e o Working Group on Women da da ISfTeH - International Society for Telemedicine and eHealth.

Bárbara Simão

Mestre em direito e desenvolvimento pela Fundação Getúlio Vargas (FGV Direito SP) e graduada pela Faculdade de Direito da Universidade de São Paulo. Durante a graduação, foi aluna intercambista na universidade Paris 1 Panthéon-Sorbonne. Atuou como pesquisadora na área de direitos digitais do Instituto Brasileiro de Defesa do Consumidor (Idec), como coordenadora de pesquisa da área Privacidade e Vigilância do InternetLab, e foi conselheira do projeto "Proteção de dados em serviços de saúde digital" da Icict/Fiocruz. Atualmente, é programme officer na Article 19.

Camila Leite Contri

Doutoranda em Direito Comercial na USP, Mestra em Direito Econômico pela Universidade Jean Moylin Lyon 3 e Bacharel em Direito pela USP e pela Universidade Jean Moulin Lyon 3. Professora na Pós Graduação de Direito Digital e

Proteção de Dados do IDP. Coordenadora do Programa de Telecomunicações e Direitos Digitais no Idec - Instituto de Defesa de Consumidores. É também uma das líderes do C20 para temas de digitalização e tecnologia e coordenadora dos livros "Dados, Mercados Digitais e Concorrência" e "Perspectivas e controvérsias na inovação regulatória no sistema financeiro de pagamentos".

Fabiana Dias

Enfermeira sanitarista, com Graduação e Licenciatura em Enfermagem na Universidade Federal Fluminense (UFF). Residência em Saúde da Família e Especialização em Saúde Pública na Escola Nacional de Saúde Pública Sérgio Arouca, da Fundação Oswaldo Cruz (ENSP/Fiocruz). Mestra em Saúde Pública (ENSP/Fiocruz) e Doutoranda no Programa de Pós-Graduação em Informação e Comunicação em Saúde do Instituto de Comunicação e Informação Científica e Tecnológica em Saúde (PPGICS/Icict/Fiocruz). Trabalhadora do Sistema Único de Saúde (SUS), integra a Equipe de Assessoria Técnica de Planejamento da Secretaria Municipal de Saúde do Rio de Janeiro (SMS-Rio). Atua no serviço, gestão, ensino e pesquisa, na área de Saúde Coletiva com ênfase em Atenção Primária à Saúde. E-mail: fabiana.cassiel@gmail.com.

Fernanda Bruno

Professora titular do Programa de Pós-Graduação em Comunicação e Cultura e do Instituto de Psicologia da UFRJ. É coordenadora do MediaLab.UFRJ, pesquisadora do CNPq e membro-fundadora da Rede latino-americana de estudos em vigilância, tecnologia e sociedade/LAVITS.

Giliate C. Coelho Neto

Médico sanitarista e Mestre em Saúde Coletiva (Unifesp). Foi diretor do Datasus e Secretário Executivo de Regulação

em Saúde da SES-PE. Atualmente atua como diretor de TI e Saúde Digital da Empresa Brasileira de Serviços Hospitalares (Ebserh).

Helena Strecker

Mestranda em Comunicação e Cultura do PPGCOM/UFRJ, pesquisadora do MediaLab.UFRJ e bolsista FAPERJ. Graduada em Psicologia pela UFRJ, pesquisa as relações entre tecnologia e subjetividade.

Jonas C. L. Valente

Pesquisador do Instituto de Internet de Oxford, onde integra o projeto Fairwork, coordenando pesquisa internacional sobre trabalho decente em plataformas online. É integrante de laboratórios e grupos de pesquisa na Universidade de Brasília, na Universidade Federal do Ceará e na Universidade Federal de Sergipe. É autor de livros sobre regulação das comunicações e da Internet, incluindo liberdade de expressão, acesso, concorrência e proteção de dados. Graduado em comunicação, tem mestrado em Políticas de Comunicação e doutorado em Sociologia pela Universidade de Brasília.

Juliana Pacetta Ruiz

Advogada em proteção de dados e regulação de tecnologia, formada pela Faculdade de Direito da Universidade de São Paulo (USP) e mestre em Administração Pública e Governo pela Fundação Getúlio Vargas-São Paulo.

Manuela Caputo

Mestranda em Comunicação e Cultura no PPGCOM/UFRJ e pesquisadora no MediaLab.UFRJ. Graduada em Comunicação Social - Jornalismo pela UFRJ. Pesquisa as relações entre tecnologia e sociedade. No terceiro setor, atua pelo acesso a informações públicas.

Maria Luciano

Bacharela e mestre em Direito (USP). Participou do Digital Identity in Time of Crisis: Designing for Better Futures Research Sprint no Berkman Klein Center, Harvard University, e da iniciativa Universal Safeguards for Inclusive DPI da ONU. Foi líder de equipe no Oxford COVID-19 Government Response Tracker na Blavatnik School of Government, University of Oxford. Consultora em Infraestruturas Públicas Digitais para instituições como o Instituto Brasileiro de Defesa de Consumidores (Idec) e o Centre for Digital Public Infrastructure (CDPI). Atualmente, é professora de governança de dados no setor público no Data Privacy Brasil, e fellow em governança participativa de dados na Connected by Data.

Mariana Martins de Carvalho

Doutora em Comunicação pela Universidade de Brasília (UnB). Com mestrado e graduação em Comunicação Social pela Universidade Federal de Pernambuco (UFPE). É gestora em comunicação da Empresa Brasil de Comunicação (EBC) e foi Coordenadora Executiva da Pesquisa Proteção de Dados Pessoais em Serviços de Saúde Digital.

Marina Fernades de Siqueira

Bacharel em direito pela Universidade São Judas Tadeu (USJT), com passagem pela Universidad Finis Terrae (UFT/Chile). Advogada e pesquisadora do programa de telecomunicações e direitos digitais do Idec - Instituto de Defesa de Consumidores. Membra da Câmara Técnica de Saúde Digital e Comunicação em Saúde do Conselho Nacional de Saúde (CTSDCS/CNS).

Matheus Z. Falcão

Doutorando e Mestre em direito pela USP. Co-diretor do Centro Brasileiro de Estudos de Saúde (Cebes). Pesquisador associado do Centro de Pesquisa em Direito Sanitário da

USP (Cepedisa). Pesquisador do projeto Saúde Amanhã, da Fiocruz. Visiting Researcher no Centre for Law, Technology and Society da Universidade de Ottawa (Canadá) e membro da Câmara Técnica de Saúde Digital e Comunicação em Saúde do Conselho Nacional de Saúde (CTSDCS/CNS).

Natália Fazzioni

Doutora em Antropologia Cultural (UFRJ, 2018), atuando principalmente nos seguintes temas: saúde, cuidado, cidades, favelas e políticas públicas. Realizou estágio de pós-doutorado no Laboratório de Comunicação e Saúde e no Programa de Pós-graduação em Informação e Comunicação em Saúde (ICICT/FIOCRUZ) e foi bolsista do projeto Proteção de Dados Pessoais em Serviços de Saúde Digital (Fiocruz/IDEC/Intervozes).

Olívia Bandeira

Doutora em Antropologia Cultural pelo Programa de Pós-Graduação em Sociologia e Antropologia da Universidade Federal do Rio de Janeiro (PPGSA/UFRJ) e mestre em Comunicação pelo Programa de Pós-Graduação em Comunicação da Universidade Federal Fluminense (PPGCOM/UFF). Possui graduação em Comunicação Social pela mesma instituição. Faz parte da Coordenação Executiva do Intervozes - Coletivo Brasil de Comunicação Social e compõe a Coordenação Geral da Pesquisa Proteção de Dados Pessoais em Serviços de Saúde Digital.

Paula Cardoso Pereira

Pós-doutoranda do Programa de Pós-Graduação em Comunicação e Cultura da UFRJ e doutora pelo mesmo programa. É pesquisadora do MediaLab.UFRJ. Desenvolve pesquisas sobre tecnologia, sociedade e subjetividade com ênfase em temporalidades algorítmicas.

Paulo Faltay

Pesquisador de Desenvolvimento Científico e Tecnológico Regional no Programa de Pós-Graduação em Comunicação da UFPE e doutor em Comunicação e Cultura pelo PPGCOM/UFRJ. Coordenador do Estopim - Laboratório em Tecnopolítica, Comunicação e Subjetividade na UFPE. Pesquisa as relações entre tecnologia, comunicação e sociedade.

Paulo Victor Melo

Pesquisador do Instituto de Comunicação da Universidade Nova de Lisboa (ICNOVA), professor de Ciências da Comunicação do IADE — Faculdade de Design, Tecnologia e Comunicação/Universidade Europeia, em Lisboa, Portugal. Doutor em Comunicação e Cultura Contemporâneas pela Universidade Federal da Bahia (UFBA). Integrante do Centro de Comunicação, Democracia e Cidadania da UFBA. Associado ao Intervozes — Coletivo Brasil de Comunicação Social

Rodrigo Murtinho

Doutor e Mestre em Comunicação pela Universidade Federal Fluminense (UFF), é pesquisador do Instituto de Comunicação e Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz), onde foi Diretor entre 2017 e 2025. Participa do Grupo de Trabalho de Comunicação e Saúde, da Associação Brasileira de Saúde Coletiva (GTCom/Abrasco), Compõe o corpo docente do Programa de Pós-Graduação em Informação e Comunicação em Saúde (PPGICS/Icict/Fiocruz), a Câmara Técnica de Saúde Digital e Comunicação em Saúde do Conselho Nacional de Saúde (CTSDCS/CNS) e o Subcomitê LGPD do Comitê Gestor de Saúde Digital, da Secretaria de Informação e Saúde Digital, do Ministério da Saúde (CGSD/SEIDIGI/MS).

Rosana Castro

Professora adjunta do Instituto de Medicina Social Hesio Cordeiro da Universidade do Estado do Rio de Janeiro (IMS/UERJ) e docente do Programa de Pós-Graduação em Saúde Coletiva do IMS/UERJ. É cientista social, mestra e doutora em Antropologia Social pela Universidade de Brasília. Autora do livro "Economias políticas da doença e da saúde: uma etnografia da experimentação farmacêutica" (2020) e co-organizadora da coletânea "Antropologias, saúde e contextos de crise" (2018). Atualmente, investiga negacionismos e práticas científicas e biomédicas envolvendo vacinas e medicamentos no contexto da pandemia de Covid-19.

Sérgio Amadeu da Silveira

Professor associado da Universidade Federal do ABC (UFABC). É pesquisador do CNPq /Produtividade em Pesquisa – 2. Fez graduação em Ciências Sociais, mestrado e doutorado em Ciência Política na Universidade de São Paulo (2005). É membro do Comitê Científico Deliberativo da Associação Brasileira de Pesquisadores em Cibercultura (ABCiber). Integrou o Comitê Gestor da Internet no Brasil (2003-2005 e 2017-2020). Coordenou o Governo Eletrônico da Prefeitura de São Paulo e criou o projeto Telecentros-SP (2001-2002). Presidiu o Instituto Nacional de Tecnologia da Informação (2003-2005). Pesquisa as implicações tecnopolíticas dos sistemas algoritmos; Inteligência Artificial e ativismo; práticas colaborativas na Internet. Integra a rede de pesquisadores Tierra Común. Autor dos livros: Democracia e os códigos invisíveis: como os algoritmos estão modulando comportamentos e escolhas políticas (2019); Tudo sobre tod@s: redes digitais, privacidade e venda de dados pessoais (2017); Exclusão Digital: a miséria na era da informação (2001); Software Livre: a luta pela Liberdade do conhecimento (2003); entre outros.

Tarcízio Silva

Senior Tech Policy Fellow pela Fundação Mozilla, e realiza pesquisa e incidência sobre transparência, responsabilidade e antirracismo na inteligência artificial. É curador na Desvelar, colaborador na Tecla/Ação Educativa e no Instituto Sumaúma. Pesquisador, mestre em Comunicação e Cultura Contemporâneas pela Universidade Federal da Bahia (UFBA); realiza doutorado em Ciências Humanas e Sociais na Universidade Federal do ABC (UFABC), onde estuda controvérsias multissetoriais na regulação de inteligência artificial.

Vanessa de Lima e Souza

É mestre em Saúde Pública e doutorada em Governação, Conhecimento e Inovação, bem como em Informação e Comunicação em Saúde. Possui 15 anos de experiência em temas relacionados com saúde digital, dados e informação em saúde, telessaúde e inteligência artificial aplicada à Saúde. Atualmente é gestora de projetos dos Serviços Partilhados do Ministério da Saúde, em Portugal. Tem se dedicado ao Espaço Europeu de Dados de Saúde e sua implementação no país, participando de grupos de trabalho técnicos europeus e nacionais. Adicionalmente, gerencia a implementação do Data Lake, repositório de dados transversal ao sistema de saúde público e privado de saúde português para fins de investigação, desenvolvimento e inovação e coordena a gestão da cedência de dados de saúde para uso secundário.

Este livro foi editado em acesso aberto, podendo ser baixado e acessado *online* em *tablets, smartphones,* telas de computadores e em leitores de *ebooks*.

Produção Multimeios | Icict | Fiocruz

Textos compostos em Acumin Pro.

Rio de Janeiro, agosto de 2025.

ISBN 978-65-87663-22-7

idec intervozes ICICT FIOCRUZ