PROTEÇÃO DE DADOS PESSOAIS EM SERVIÇOS DE SAÚDE DIGITAL

Aqui somos SUS

# RESUMO EXECUTIVO

## Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil

ICICT Instituto de Comunicação e Informação Científica e Tecnológica em Saúde

Ministério da Saúde
FIOCRUZ
Fundação Oswaldo Cruz

idec
Instituto Brasileiro de Defesa do Consumidor

intervozes
coletivo brasil de comunicação social

# RESUMO EXECUTIVO

## Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil

OUTUBRO | 2022

# EXPEDIENTE

## Realização

Instituto de Comunicação Informação Científica e Tecnológica em Saúde, da Fundação Oswaldo Cruz (Icict/Fiocruz)
Intervozes – Coletivo Brasil de Comunicação Social
Instituto Brasileiro de Defesa do Consumidor (Idec)

## Coordenação Geral

Rodrigo Murtinho - Icict/Fiocruz
Aldo Pontes - Icict/Fiocruz
Marcelo Fornazin - Escola Nacional de Saúde Pública (ENSP/ Fiocruz)
Olívia Bandeira - Intervozes
Matheus Z. Falcão - Idec

## Coordenação Executiva e de Pesquisa

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 - *Dept. de Direitos Humanos da Escola Nacional de Saúde Pública Sergio Arouca (DIHS/ENSP/ Fiocruz) e Pós-graduação Stricto sensu em Ensino em Biociências e Saúde do Instituto Oswaldo Cruz (PGEBS/IOC/Fiocruz)*

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

Bárbara Simão - *Mestranda 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 Coelho - *Médico Sanitarista e pesquisador em Saúde Coletiva com especialização em Medicina de Família e Comunidade (UPE)*

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*

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

Paulo Rená - *Aquatune Lab*

Rosana Castro - *Professora adjunta do Instituto de Medicina Social da Universidade do Estado do Rio de Janeiro.*

Stephan Sperling - *Médico Assistente e Tutor do Programa de Residência em Medicina de Família e Comunidade da Faculdade de Medicina da (USP)*

Tarcízio Silva - *Senior Tech Policy Fellow na Mozilla Foundation e Doutorando PCHS-UFABC*

## Projeto gráfico e diagramação

Valéria Sá - Icict/Fiocruz


## Apoio:

Diabete Brasil

Este projeto foi financiado por emendas parlamentares dos deputados federais Fernanda Melchionna (PSOL/RS) e Luciano Ducci (PSB/PR).



Este trabalho está licenciado com uma Licença Creative Commons Attribution-ShareAlike 4.0 Internacional (CC BY-SA 4.0) https://creativecommons.org/licenses/by-sa/4.0/

# SUMÁRIO

1 - APRESENTAÇÃO 07

2 - A DIGITALIZAÇÃO DA SAÚDE: OPORTUNIDADES E RISCOS 09

3 - METODOLOGIA 12

4 - RESULTADOS 14

4.1 - A PESQUISA BIBLIOGRÁFICA 14

4.2 - LEVANTAMENTO DOCUMENTAL 16

4.3 - ENTREVISTAS 19

4.4 - INVENTÁRIO DE TECNOLOGIAS DIGITAIS EM SERVIÇOS DE SAÚDE 29

5 - LACUNAS REGULATÓRIAS E OS DESAFIOS PARA O DIREITO À PROTEÇÃO DE DADOS PESSOAIS EM SERVIÇOS DE SAÚDE 39

# 1 APRESENTAÇÃO

O projeto Proteção de Dados Pessoais em Serviços de Saúde Digital tem o objetivo de contribuir para a compreensão dos sistemas e processos de digitalização dos serviços de saúde e de tratamento de dados pessoais em serviços de saúde e para o fortalecimento da cultura de proteção de dados pessoais na área da saúde, tendo como referência a Lei Geral de Proteção de Dados (LGPD), aprovada em 2018.

O projeto surgiu em um cenário de rápido crescimento do uso de tecnologias da informação e comunicação e de coleta e tratamento de dados pessoais no campo da saúde. Tal expansão foi reforçada pelo contexto da pandemia da Covid-19, que tornou este estudo ainda mais atual e urgente. Nos últimos anos, houve grande disseminação de aplicações e serviços digitais, com o uso de dados pessoais sensíveis, tanto no SUS quanto nos serviços privados.

Entende-se que o uso das novas tecnologias de informação e comunicação no campo da saúde trazem oportunidades, mas também riscos no que se refere à proteção de dados pessoais que precisam ser mais bem investigados para que boas práticas sejam construídas.

## ASSIM, A PESQUISA BUSCOU ATUAR EM QUATRO ETAPAS:

1) Levantar e analisar a produção científica mais recente sobre as implicações e os impactos das tecnologias no sistema de saúde, em relação com a regulação das práticas de proteção de dados pessoais, a partir de uma revisão integrativa de literatura;

2) Compreender como os governos e corporações estão formulando e operacionalizando regulações a respeito do uso de dados pessoais na saúde, a partir de uma pesquisa documental sobre leis, normas e recomendações nacionais e internacionais sobre o assunto;

3) Compreender as percepções de usuários/as, profissionais e gestores/as de sistemas públicos e do setor privado acerca do tema proteção de dados pessoais e conhecer algumas das principais tecnologias por eles utilizadas;

4) Construir um inventário de tecnologias digitais, com base nas entrevistas e revisão bibliográfica, com vistas a identificar práticas de coleta, armazenamento e tratamento de dados de saúde relevantes para a compreensão do comportamento do setor.

Para compreender as percepções dos/as usuários/as, profissionais e gestores/as da saúde, foram realizadas 33 entrevistas semiestruturadas com usuários/as dos sistemas de saúde público e privado que convivem com doença crônica (diabetes), profissionais de saúde diretamente envolvidos com atenção em saúde e/ou coleta de dados em saúde, gestores/as da saúde no município de Recife (PE), representantes do Conselho Federal de Medicina (CFM) e da Associação Brasileira de Planos de Saúde (Abramge). A percepção desses agentes é fundamental para a compreensão dos benefícios e riscos da digitalização da saúde no que se refere à proteção de dados pessoais e para a formulação de políticas públicas que considerem essa proteção como um direito.

Entre os principais resultados, a pesquisa identificou que há uma lacuna na literatura, sobretudo nacional, no que diz respeito à centralidade do/a usuário/a, que é o titular dos dados, nas análises sobre proteção de dados na saúde. Sabe-se pouco sobre o perfil e a percepção dos/as usuário/as de serviços de saúde digital, no tocante à proteção de dados.

Observou-se também, em diferentes relatos, a importância do acesso à informação para, dentre outras coisas, fortalecer o exercício do direito à proteção de dados pessoais.

Chamou atenção o crescente uso de tecnologias da informação e da comunicação voltados para saúde e a quantidade de dados coletados, sistematizados e muitas vezes compartilhados cotidianamente. Há também uma significativa apropriação de outros tipos de plataformas, como redes sociais e serviços de mensageria, para mediação dos serviços de Saúde Digital, o que deixa ainda mais complexa e necessária a regulamentação infralegal e a fiscalização do setor, tornando urgente a definição do que são dados de saúde, e que configuram dados pessoais sensíveis, para que haja a segurança adequada desse tipo de dado.

Uma ampla maioria de entrevistados/as afirmou participar de programas de fidelização de farmácias e laboratórios, ao mesmo tempo em que declarou ter receio quanto ao compartilhamento dos seus dados pessoais. A falta de transparência na coleta, no tratamento e no compartilhamento de dados além de gerar dúvidas nos/as usuários/as, gera insegurança e sensação de impotência e de irreversibilidade da perda de controle sobre o fluxo dos seus dados. A preocupação dos/as entrevistados/as revela, portanto, que os/as usuários/as brasileiros/as não estão alheios à discussão sobre proteção de dados pessoais, mas parecem se sentir de "mãos atadas" diante da "troca" pouco transparente de dados por descontos, por exemplo.

O Inventário de Tecnologias Digitais que coletam dados em serviços de Saúde Digital contribuiu ainda para consolidar as percepções dos/as usuário/as na medida em que a análise em profundidade das tecnologias selecionadas revelou que a maioria delas oferece mecanismos considerados pouco transparentes para os/as usuários/as e, sobretudo, baseados em noções de consentimento bastante frágeis, tendo em vista a complexidade do mercado de dados e das interações existentes entre tecnologias, governos e grandes corporações.

A garantia da proteção de dados dos/as usuários/as enfrenta barreiras também no que se refere às normas. Em primeiro lugar, observou-se uma ausência de diálogo entre os textos das normas analisadas. Há também pouca uniformidade (ou imprecisão) na nomenclatura adotada para se referir à proteção de dados, e as discussões sobre dados pessoais são abordadas muitas vezes pela lógica do sigilo (sigilo médico), desconsiderando como os dados circulam a partir do uso das tecnologias. As normas e documentos analisados também promovem confusão entre privacidade e proteção de dados pessoais, e a segurança costuma ser tratada de forma geral e superficial, sendo descrita muitas vezes como sinônimo de "cibersegurança".

Esses resultados estão agrupados em uma série de produtos que têm como objetivo contribuir com o aprofundamento da discussão conceitual sobre a proteção de dados pessoais nos serviços de Saúde Digital, para a estruturação de normas e boas práticas que ajudem a garantir a proteção no cotidiano dos itinerários de saúde e para efetivar a proteção de dados como um direito dos/as usuários/as. Entre os produtos do projeto temos o **Relatório Proteção de Dados Pessoais em Serviços de Saúde Digital** com os resultados completos da pesquisa, uma Coletânea de artigos escritos pela equipe da pesquisa e por pesquisadores e especialistas convidados, um **Guia para Profissionais da Saúde** sobre proteção de dados pessoais em serviços de Saúde Digital e uma **Campanha** informativa sobre proteção de dados em Saúde Digital, voltada para os/as usuários/as, profissionais e gestores/as e disseminada nas redes sociais. Todo o material está disponível na página do projeto (link).

# 2 A DIGITALIZAÇÃO DA SAÚDE: OPORTUNIDADES E RISCOS

O direito à proteção de dados pessoais é fundamental diante de uma sociedade cada vez mais permeada pela plataformização (Zuboff[1], 2021, Van Djick, Poell, 2016[2]) das esferas da vida e a geração de um significativo mercado de dados pessoais. Na saúde, 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. A pandemia não apenas acelerou o uso de tecnologias quanto ensejou a regulamentação e permissão de práticas digitais na saúde, como a telessaúde e a prescrição eletrônica. Essa nova realidade fez com que os dados de saúde - considerados sensíveis e, portanto, merecedores de cuidados adicionais pela LGPD - passassem a trafegar de forma cada vez mais rápida e desafiadora para as autoridades públicas responsáveis pela fiscalização.

Algumas das práticas mapeadas pela pesquisa que estão associadas à Saúde Digital e que coletam e tratam dados pessoais são: uso de prontuários e de prescrições eletrônicas, uso de dispositivos portáteis de saúde, aplicativos de automonitoramento, plataformas de teleconsulta, serviços de mensageria (como o Whatsapp), redes sociais, entre outros.

Parte dessas ferramentas servem a ações e a serviços fundamentais dentro do sistema de saúde. No campo da saúde pública, que desenvolve ações em escala populacional, a coleta e o tratamento de dados é um instrumento indispensável para a vigilância em saúde. Já no campo dos serviços de saúde, tanto públicos quanto privados, há um conjunto cada vez maior de soluções digitais para reduzir custos e otimizar a eficácia e a qualidade do tratamento. Essas soluções englobam tanto a telessaúde[3], que possibilita a assistência terapêutica à distância, quanto medidas que combinam inteligência artificial com o uso de dados para otimizar fluxos de atendimento, realizar análises individualizadas de risco e prescrever comportamentos (Patz, Piaia, 2021[4]; OMS, 2021)[5]. Os dados pessoais coletados nos serviços de saúde são frequentemente utilizados também em pesquisas de novos tratamentos e medicamentos.

---

[1] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira de poder. 1a ed. Intrínseca, Rio de Janeiro. 2021.

[2] VAN DJICK, José, POELL Thomas. Understanding the promises and premises of online health platforms. Big Data & Society January–June 2016.

[3] A Telessaúde é definida pela OMS 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" (OMS, 2012). Para um debate mais amplo sobre o conceito de telessaúde, ver o relatório completo da pesquisa.

[4] PATZ, Stéfani Reimann; PIAIA, Thami Covatti. Vigilância, Perfilamento e Tratamento de Dados Pessoais no Contexto do Controle Migratório. RDP, Brasília, Volume 18, n. 100, 690-720, out./dez. 2021.

[5] WORLD HEALTH ORGANIZATION et al. Ethics and governance of artificial intelligence for health: WHO guidance. 2021.

Entretanto, se o uso das novas tecnologias de informação e comunicação no campo da saúde trazem benefícios, oportunizam igualmente riscos no que se refere à proteção de dados pessoais. As tecnologias na saúde produzem um mercado de dados pessoais sensíveis bastante complexo, que envolve trocas e arranjos entre tecnologias e empresas (Lupton, 2016[6], Palleta et al., 2021[7], Souza, 2018[8], Bruno, 2021[9]). Em grande parte das vezes, os dados pessoais são também utilizados de forma pouco transparente. As informações são de difícil acesso tanto para pesquisadores que têm buscado entender a coleta e o tratamento dos dados pessoais quanto para os usuários dos sistemas de saúde.

O uso das tecnologias pode também criar sistemas de classificação que podem afetar de maneira desproporcional as pessoas que já são discriminadas na sociedade, a partir de recortes étnico-raciais, território, de gênero, de sexualidade (Silva, 2022[10], Benjamin, 2019[11], Peña, Varon, 2019[12]) ou até mesmo a partir de condições de saúde pré-existentes e idade. Outro risco que não pode ser menosprezado é o de incidentes de segurança, por exemplo, vazamentos de dados, como os que aconteceram no Ministério da Saúde nos anos de 2020 e 2021 (Idec, 2020[13]). Os dados faziam parte de sistemas de informação sob responsabilidade do Ministério da Saúde e informações dos/as usuários/as ficaram desprotegidas, desvelando uma falha na proteção dos dados de um dos principais e mais importantes bancos de dados do país.

Para além dos riscos apontados, não há como falar em tecnologias digitais no Brasil sem falar sobre as desigualdades de acesso à internet e como isso impacta e muitas vezes fortalece as assimetrias já existentes. Conforme apresentado na Pesquisa TIC Domicílios 2020 (Cetic.br, 2021)[14] e reforçado pela pesquisa Territórios Livres, Tecnologias Livres (Intervozes, Conaq e MMTR-NE, 2021)[15] desigualdades de classe, raça e etnia, além das desigualdades regionais e entre os meios urbanos e rurais, caracterizam o acesso à internet existente no Brasil hoje. Segundo a TIC Domicílios, 12 milhões de domicílios no Brasil (17%) não possuem acesso à internet, e 55% deles não possuem computadores, principalmente nas classes sociais com menor renda familiar. Na análise feita por indivíduos, 58% dos brasileiros e brasileiras entrevistados/as que declararam ter acesso à internet acessam a rede apenas pelo celular. Esse número cresce em áreas rurais e entre os que se declaram pretos, pardos ou indígenas.

---

[6] LUPTON, Deborah. The quantified self. Malden: Polity, 2016.

[7] PALETTA, Gabriela et al. "Aplicativos de monitoramento do ciclo menstrual e da gravidez: corpo, gênero, saúde e tecnologias da informação". Cadernos Pagu, 2020.

[8] SOUZA, Joyce. "A saúde dos dados pessoais e o município de São Caetano do Sul". Dissertação apresentada ao Programa de Pós-graduação em Ciências Humanas e Sociais da UFABC, 2018.

[9] BRUNO, Fernanda et al. "Tudo por conta própria": autonomia individual e mediação técnica em aplicativos de autocuidado psicológico". Reciis – Revista Eletrônica de Comunicação, Informação & Inovação em Saúde, Rio de Janeiro, v. 15, n. 1, p. 33-54, jan./mar. 2021.

[10] SILVA, Tarcizo. Racismo algorítmico: inteligência artificial e discriminação nas redes digitais. Edições Sesc SP; 1ª edição, 2022.

[11] BENJAMIN, Ruha. Race After Technology: Abolitionist Tools for the New Jim Code (2019).

[12] PEÑA, Paz; VARON, Joana. Decolonising AI: A transfeminist approach to data and social justice. Disponível em: https://giswatch.org/sites/default/files/gisw2019_artificial_intelligence.pdf

[13] "Vazamentos de dados de saúde coloca consumidor em risco; veja o que fazer" (IDEC,22/12/2020). Disponível em: https://idec.org.br/noticia/vazamentos-de-dados-de-saude-coloca-consumidor-em-risco-veja-o-que-fazer. Acesso em 6 out 22.

[14] 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/

[15] Resultados disponíveis em: http://territorioslivres.online/ Acesso em 14 out. 22

De acordo com a Organização das Nações Unidas (ONU, 2021[16]), a população mundial que não tem acesso à internet está em desvantagem profunda, não apenas no acesso à informação, mas no acesso à educação, saúde, possibilidades de trabalho e formas de compensar a crise econômica. Uma pesquisa do Idec e do Instituto Locomotiva indicou que a falta de acesso à internet é uma barreira crescente para acesso a serviços públicos digitalizados por populações de menor renda[17]. Outro problema relevante é que muitos não têm um acesso que seja bom o suficiente para usufruir da educação à distância, informações de saúde ou simplesmente informação geral sobre o estado do país, negócios, etc., trazendo implicações na garantia dos direitos sociais.

No campo da saúde, a desigualdade faz com que uma parcela considerável da população não tenha acesso aos benefícios da digitalização na área. Também viola o direito dos/as usuários/as em receber e em produzir informações. Tal situação dificulta a participação social no acompanhamento e na formulação de políticas públicas de saúde, elemento essencial para a garantia desse direito, como mostra o histórico de desenvolvimento do SUS. Também dificulta a compreensão do uso que é feito de seus dados por serviços presenciais e digitais de saúde.

**Dessa forma, a desigualdade de acesso às tecnologias de informação e comunicação e à internet e a necessidade de proteção de dados pessoais sensíveis trazem novos elementos para o debate sobre o direito à comunicação como essencial também para a garantia do direito à saúde[18].**

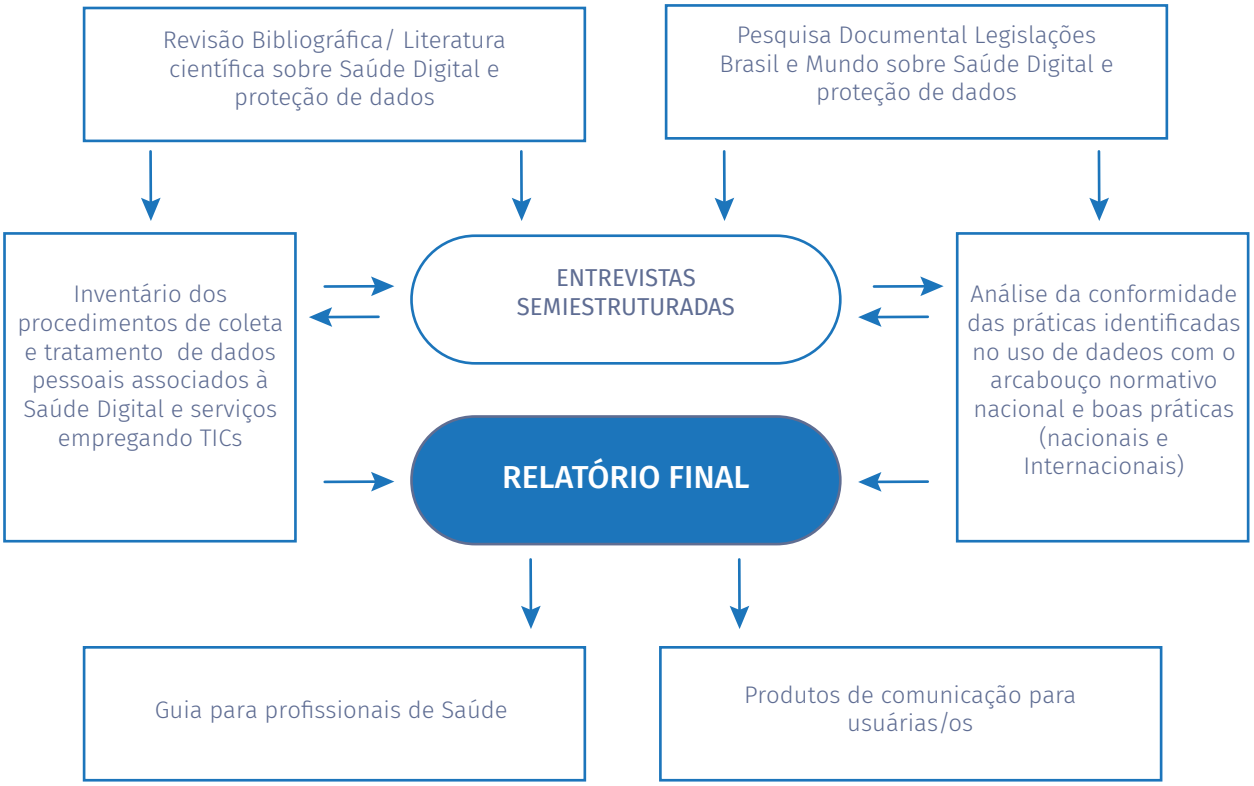
[16] Relatório divulgado pela "União Internacional das Telecomunicações". Disponível em: https://brasil.un.org/pt-br/161450-29-bilhoes-de-pessoas-nunca-acessaram-internet . Acesso em 14 out. 22.

[17] IDEC, Instituto Locomotiva; Acesso a internet móvel pelas classes C e D. 2021. Disponível em: <https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf>. Acesso em 14 out. 22.

[18] Sobre o tema, consultar: STEVANIM, Luiz Felipe; MURTINHO, Rodrigo. Direito à Comunicação e Saúde. Rio de Janeiro: Editora Fiocruz, 2021.

# 3 METODOLOGIA

o projeto atuou em quatro frentes para alcançar seus objetivos, foram elas: a revisão bibliográfica, a pesquisa documental, as entrevistas e o inventário de tecnologias. A imagem abaixo representa o fluxo realizado entre as etapas e os resultados.




## CADA UMA DAS ETAPAS SE UTILIZOU DE UMA METODOLOGIA ESPECÍFICA

**REVISÃO BIBLIOGRÁFICA:** foi feita a partir de três bases de dados (BVS, Google Acadêmico e OASIS), considerando os períodos de 2014 a 2021, tendo como referência temporal o Marco Civil da internet. foram selecionados para a fase de análise 82 estudos, dentre 468 encontrados. o roteiro de análise dos textos contemplou questões relacionadas à utilização das tecnologias de Informação e Comunicação (TIC's) nos serviços de saúde e o processo de proteção dos dados nesses serviços, pensando a instituição de boas práticas de segurança da informação, privacidade

e confidencialidade dos dados, identificação dos riscos e vulnerabilidades referentes a coleta e tratamento dos dados inclusive no âmbito farmacêutico, os agentes envolvidos nessa prática, a percepção dos usuários, profissionais e gestores, além dos marcos legais quanto a proteção dos dados e conflitos éticos no uso das informações em saúde.

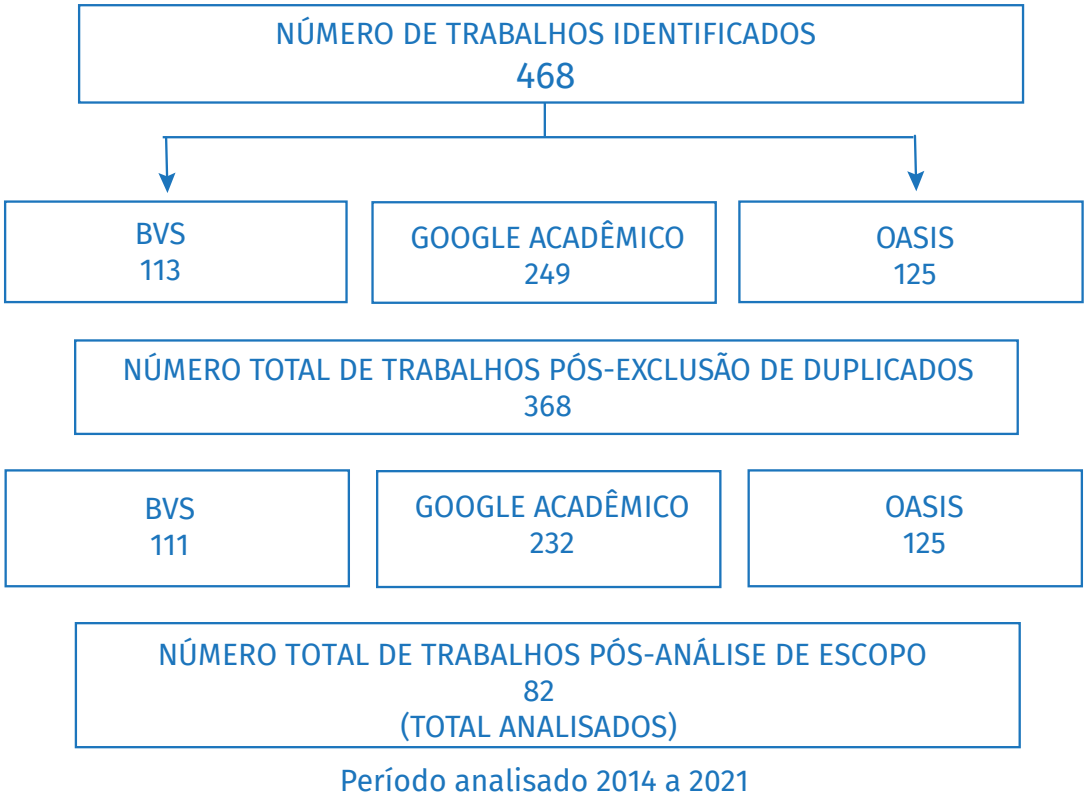
**REVISÃO DOCUMENTAL:** no que diz respeito às legislações nacionais, a pesquisa foi realizada em bases de dados de órgãos do Governo Federal e de conselhos federais da área de saúde. Já em relação aos padrões internacionais, a pesquisa buscou mecanismos regulatórios dos principais órgãos multilaterais e regionais na área da saúde. Foram analisados 88 documentos relativos a proteção de dados e regulação em saúde, sendo 60 de âmbito nacional (Brasil) e 28 internacionais (regionais e outros países).

**ENTREVISTAS:** foram conduzidas 28 entrevistas semiestruturadas e um grupo focal com cinco pessoas. As entrevistas tiveram como foco: a) gestores/as da Prefeitura do Recife, da Secretaria de Saúde e da Gerência de Tecnologia de Saúde da cidade; b) profissionais de saúde diretamente envolvidos com atenção em saúde e/ou coleta de dados em saúde também do território selecionado; c) representantes de conselhos profissionais, especialmente de medicina; d) representantes de prestadores de saúde; e) usuários/as com doença crônica (diabetes), uma vez que costumam utilizar tecnologias em seu cotidiano de tratamento de saúde. Os/as usuários/as foram divididos em três subgrupos: usuários/as comuns, influenciadores digitais e membros da Associação de Diabetes Juvenil - ADJ. As entrevistas foram realizadas por meio da plataforma Zoom e gravadas mediante consentimento.

**INVENTÁRIO DE TECNOLOGIAS:** teve como base os resultados do levantamento bibliográfico e das entrevistas. Foram incluídas tanto as tecnologias citadas nos trabalhos analisados (108 tecnologias), quanto as mencionadas nas entrevistas (30 tecnologias), totalizando 138 tecnologias, das quais 50 foram categorizadas e analisadas em primeiro nível e 12 foram selecionadas para uma análise em profundidade que avalia a conformidade das práticas identificadas no uso de dados com o arcabouço normativo nacional e de boas práticas.

# 4 RESULTADOS

## 4.1 A PESQUISA BIBLIOGRÁFICA




Período analisado 2014 a 2021

A pesquisa bibliográfica se utilizou de três bases de dados, sendo uma delas latinoamericana, uma nacional e outra internacional. Ao analisar os resultados, constatou-se uma maior presença de estudos nacionais, provavelmente devido aos termos de busca que contemplaram a Lei Geral de Proteção de Dados, além de duas das bases (BVS e OASIS) conterem sobretudo trabalhos nacionais.

Dentre os estudos selecionados para a análise, 78,3% foram publicados por pesquisadores de origem nacional, e 19,3% internacional, resultando em 85,5% das publicações no idioma português. Em relação aos pesquisadores de origem nacional, a região Sudeste concentra o maior número: 42,2% dos pesquisadores estão vinculados a instituições de ensino ou grupo de pesquisa nessa região do país, seguido da região Sul com 28,1% e da região Nordeste com 15,6%.

As principais áreas de atuação dos pesquisadores se concentram nas Ciências Jurídicas (47%) e nas Ciências da Saúde (31,3%). A área de conhecimento das publicações também reflete esse cenário, onde 42,1% dos estudos foram publicados em revistas na área das Ciências da Saúde e 40,4% na área das Ciências Jurídicas.

Quanto ao gênero dos pesquisadores, 53,3% são do sexo masculino e 46,7% do sexo feminino. Apesar do recorte temporal ter início em 2014, o período de 2018 a 2021 concentrou as publicações nessas áreas de conhecimento. Quanto ao tipo de texto, 61,4% são artigos publicados em revistas científicas e 20,5% dissertações de mestrado.

Quanto aos sistemas de saúde, 28,4% abordaram o sistema de saúde público; 9,9% o sistema de saúde privado; e 30,9% abordaram ambos os sistemas de saúde. Apenas 14,5% dos estudos abordaram o tema sobre a coleta e o tratamento de dados pessoais no varejo farmacêutico.

## TEMAS E ABORDAGENS

As principais palavras-chaves encontradas nos estudos e que apresentaram o maior número de repetições caracterizam os principais temas que aparecem nos textos levantados. São eles, nessa ordem:

- tecnologia(s)
- saúde
- proteção de dados (pessoais)
- confidencialidade
- dados pessoais ou dados pessoais sensíveis
- privacidade
- telemedicina
- Covid-19

Em termos conceituais, os artigos analisados debruçaram-se sobretudo em torno das seguintes categorias: Saúde Digital; Telemedicina; Telessaúde; Proteção de Dados Pessoais; Privacidade. O debate em torno dessas categorias pode ser visto no relatório final completo da pesquisa (link). Destacamos, contudo, a ausência de uma única definição para esses termos e a importância do debate em torno deles em futuras pesquisas.

**A pesquisa identificou que 78% dos estudos fizeram menção aos riscos e vulnerabilidades relacionados ao tema de Saúde Digital e proteção de dados pessoais**. Entre os riscos e vulnerabilidades estão compreendidos aspectos como a ausência de uma política nacional de segurança dos dados, implicando em questões sobre a regulamentação e aspectos legais, permissões, consentimentos, conflitos éticos e desigualdades étnicas, sociais e econômicas quanto ao uso, acesso, coleta, tratamento, armazenamento, compartilhamento e segurança dos dado de saúde. Dentre os aspectos mais abordados para exemplificar os riscos e vulnerabilidades à proteção de dados pessoais na área da saúde, o material levantado abordou, sobretudo, os seguintes: **monetização, perfilamento de comportamento, confidencialidade, segurança e privacidade**.

Em relação às boas práticas no processo de tratamento dos dados pessoais em saúde, 69% dos estudos mencionaram ou sugeriram ações pertinentes a essa conduta. As boas práticas observadas nos textos dividem-se entre aquelas voltadas a: empresas do setor de saúde, universidades/pesquisadores, sistemas e serviços de saúde e cidadãos/consumidores. Referem-se a normas legais e responsabilidade civil dos agentes responsáveis pelos tratamentos de dados, normas legais e direitos dos cidadãos/consumidores e sistemas técnicos de gestão e segurança de dados.

**Apenas 27,7% dos estudos trouxeram informações sobre usuários/as dos sistemas de saúde e 8,4% a percepção dos/as usuários dos sistemas de saúde e dos/as gestores/as e profissionais de saúde sobre a coleta e o tratamento de dados pessoais, o que indica a ausência das percepções e perspectivas dos usuários no debate sobre proteção de dados pessoais e saúde. Outra ausência nos estudos são os marcadores sociais da diferença, relacionados à raça/etnia, gênero, sexualidade e faixa etária: somente 8,5% dos estudos trouxeram esse recort**e.

## 4.2 LEVANTAMENTO DOCUMENTAL

Foram identificados, inicialmente, 1.036 documentos, sendo 703 de legislação federal, 218 de órgãos internacionais e 115 de conselhos profissionais e agências reguladoras nacionais. Após processo de mineração e análise preliminar, totalizou-se, ao final, **88 documentos relacionados à proteção de dados pessoais em saúde, sendo 60 de âmbito nacional (Brasil) e outros 28 internacionais (regionais e outros países).**

Após leitura da legislação levantada, selecionou-se 38 documentos nacionais para análise. A maioria dos documentos são normas de conselhos profissionais (boa parte emitida pelo Conselho Federal de Medicina) e de legislação federal. Apenas 4 entre esses documentos tratam especificamente da proteção de dados por parte da administração pública[19].

Grande parte desse material foi editada/elaborada a partir de 2017 e, mais ainda, de 2018, após as promulgações do Marco Civil da Internet (Lei nº 2.965/2014) e da Lei Geral de Proteção de Dados (Lei nº 13.709/2018, com entrada em vigor em setembro de 2020), confirmando a nossa hipótese inicial de uma maior formulação legislativa e normativa sobre proteção de dados pessoais a partir de legislações federais orientadoras.

**No entanto, foi observado que, de um modo geral, 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 tratamento de dados pessoais, dentre outras medidas.**

Dos documentos que foram publicados de 2020 em diante, apenas 7 mencionam explicitamente os conceitos de "dado pessoal" ou "dado pessoal sensível" e apenas 6 mencionam explicitamente a LGPD. No entanto, a grande maioria dessas menções não traz informações adicionais e específicas em relação a como a LGPD deverá ser cumprida, e sim enuncia-se que a LGPD deverá ser observada, sem oferecer maior detalhamento.

Isso pode representar um problema, visto que apesar de a LGPD ser uma legislação bastante extensa e se aplicar para tratamentos de dados pessoais no setor público e privado, há ainda muitos pontos a serem discutidos e regulados, especialmente no que diz respeito a dados sensíveis e dados e operações de saúde.

---

[19] O Decreto nº 29/2017; (ii) a Lei nº 13.257/2016; e (iii) o Decreto nº 10.488/2020; (iv) Portaria nº 1.434/2020.

A maioria dos documentos/normas analisados tem como objetivos o estabelecimento de direitos e garantias; a criação de um órgão ou procedimento; e a descrição de situações com emissão de recomendações, o que está em sintonia com o caráter recente das legislações orientadoras citadas acima.

**A maioria dos documentos não menciona nem privacidade nem proteção de dados pessoais. Ao considerarmos apenas as normas editadas a partir de 2018 (19 normas), 12 documentos não mencionam privacidade e 7 o fazem; no que se refere à proteção de dados ou dados pessoais sensíveis, 9 documentos não mencionam esses termos, enquanto 10 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. **Nenhum dos documentos, por exemplo, diferencia de maneira expressa "privacidade" e "proteção de dados pessoais". Quando muito, há o uso desses termos com conotações diferentes mas em nenhum dos casos há preocupação em explicar o que está por detrás da diferença entre esses dois conceitos. Compreende-se aqui que essa imprecisão pouco colabora com o entendimento do conjunto da população sobre as diferenças entre os dois conceitos.**

Vale destacar que o direito à privacidade é um direito historicamente mais antigo, que surge da necessidade de garantir ao indivíduo um ambiente particular - sem interferência ou imposição de autoridade pública - para o livre desenvolvimento de sua vida e ideias. Já o direito à proteção de dados pessoais é um direito emergente, focado na autonomia individual em relação aos próprios dados e na proteção contra discriminação e mau uso, que surge a partir dos impactos da sociedade da informação (computadores, banco de dados pessoais, controle da informação) na vida dos indivíduos e a cada vez maior fonte de poder que esses dados representam (Vergilli, 2019)[20].

**Outro apontamento sobre o conjunto dos documentos e normas é a ausência, de um modo geral, de informações mais específicas sobre determinados segmentos populacionais e como critérios de raça/cor, território, gênero, idade e sexualidade são marcadores importantes também quando os assuntos são Saúde Digital e proteção de dados pessoais. Das 38 normas analisadas, apenas 5 trazem algum tipo de recorte direcionado a um público específico**.

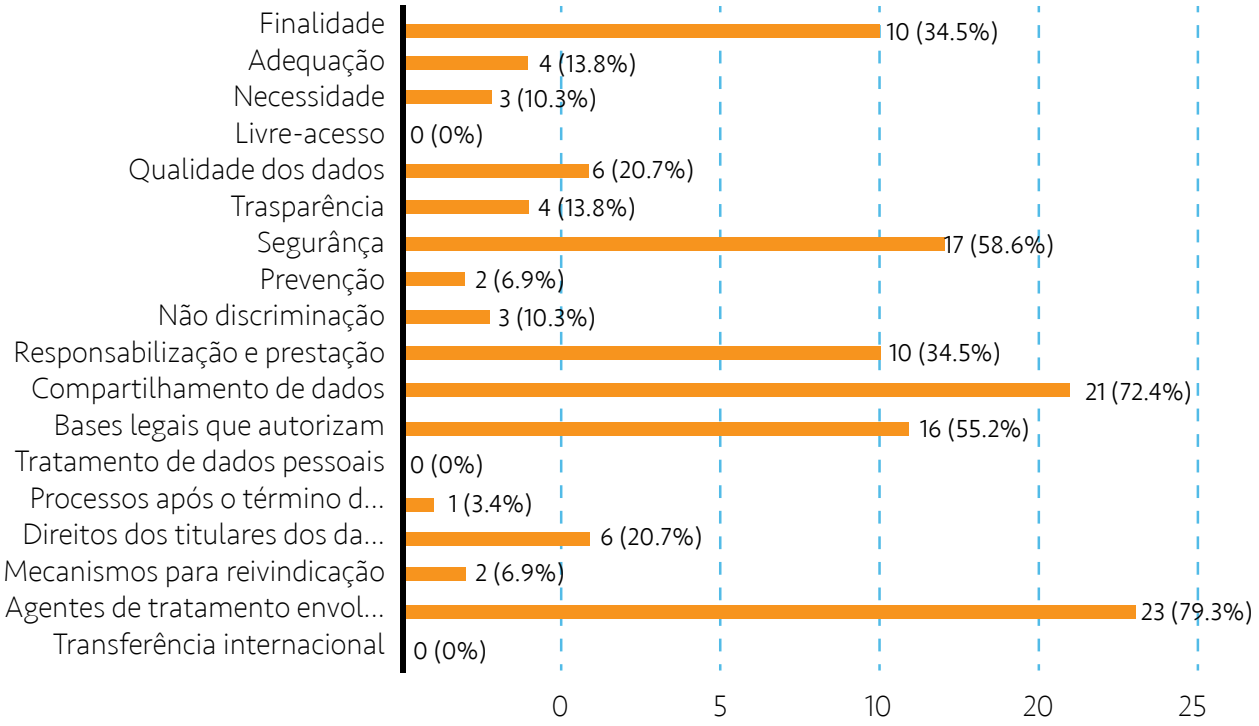
No que se refere a pontos essenciais presentes em legislações orientadoras de proteção de dados, abaixo estão listados os assuntos predominantes nos documentos (lembrando que um documento pode mencionar mais de um assunto ao mesmo tempo):

[20] VERGILLI, Gabriela. "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", 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/

## GRÁFICO 12 - "RECORTES" APRESENTADOS NO DOCUMENTO

A NORMA OU DOCUMENTO REGULAMENTA OU TANGENCIA ALGUM DOS SEGUINTES PONTOS?

29 RESPONSES




FONTE: ELABORAÇÃP PRÓPRIA

## HÁ TRÊS TEMÁTICAS PREDOMINANTES:

**1. Indicação de agentes de tratamento envolvidos na atividade:** muitas das normas indicam quais seriam os agentes de tratamento envolvidos em determinada operação (médicos, enfermeiros, instituições de saúde, dentre 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. A questão é particularmente relevante, pois a LGPD tem dispositivos específicos sobre tratamento de dados de saúde, deixando alguns conceitos carentes de regulamentação, por exemplo, tutela da saúde e autoridade sanitária. a

**2. Compartilhamento de dados:** algumas normas indicam as circunstâncias nas quais os dados poderão ser compartilhados ou simplesmente indicam que dados poderão ser compartilhados. Na maioria dos casos, as previsões são genéricas, afirmando que os agentes deverão adotar medidas relativas à segurança dos dados e preservação de seu sigilo, quando for o caso.

**3. Indicação de medidas de segurança da informação:** 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.

**Outro ponto a ser destacado é que o "consentimento" aparece de forma recorrente em diversos documentos. No universo analisado, 7 citam o consentimento como necessário para a realização de determinadas atividades.**

Dentre elas, estão: o consentimento do paciente ao médico para revelar conteúdos de seu prontuário para terceiros; o consentimento do paciente para a transmissão eletrônica de imagens de seus exames para terceiros; o consentimento para o acesso ao conhecimento tradicional associado de origem identificável[21]; e o consentimento para a pesquisa científica.

Resta a dúvida, porém, se o "consentimento"citado nessas normas seria equivalente ao consentimento como base legal da LGPD. Em casos, por exemplo, sobre o consentimento de pacientes para compartilhamento de dados de seus prontuários ou exames, poderia-se 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. 8, § 5º da LGPD determina que o consentimento 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 e a quantidade de profissionais e instituições envolvidas no fluxo dos serviços de saúde, eventualmente a transmissão eletrônica de determinados dados pode ser a única forma de prestar alguns tipos de serviço, de forma que devemos inquirir se, nesse tipo de situação, o consentimento seria realmente livre e ainda se ele seria a base legal adequada para esse tratamento.**

Chama a atenção também que apenas 3 documentos mencionam, autorizam ou definem 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. Alguns indicadores nesse sentido são 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.

## 4.3 ENTREVISTAS

Foram conduzidas 33 entrevistas semiestruturadas, sendo: 16 com usuários/as dos sistemas de saúde público e privado que convivem com uma doença crônica específica, a diabetes, 10 com profissionais de saúde diretamente envolvidos com atenção em saúde e/ou coleta de dados em saúde, 5 com gestores/as da Prefeitura do Recife, da Secretaria de Saúde e também da Gerência de Tecnologia de Saúde, 1 com representantes do Conselho Federal de Medicina, e 1 com a Associação Brasileira de Planos de Saúde.

Entre os entrevistados que responderam ao questionário socioeconômico enviado antes da realização da pesquisa encontrou-se a seguinte realidade[22]: **56% de entrevistadas/os autodeclaradas/os brancas/os, 39% pardas/os e 6% pretas/os. Já em termos de renda, 11% declarou possuir renda familiar mensal de até 2 salários mínimos, 33% de 4 a 10 salários mínimos, 11% de 10 a 20 salários mínimos e 11% acima de 20 salários mínimos**.

[21] O Decreto nº 8.772, de 2016, define origem identificável como "qualquer população indígena, comunidade tradicional ou agricultor tradicional que cria, desenvolve, detém ou conserva determinado conhecimento tradicional associado".

[22] Vale ressaltar que visando preservar os dados dos entrevistados, o questionário socioeconômico foi enviado posteriormente por meio de preenchimento anonimizado. Entretanto, nem todos os participantes aderiram ao questionário. A realidade descrita acima, portanto, refere-se a um universo de cerca de 60% dos participantes.

## USUÁRIOS/AS

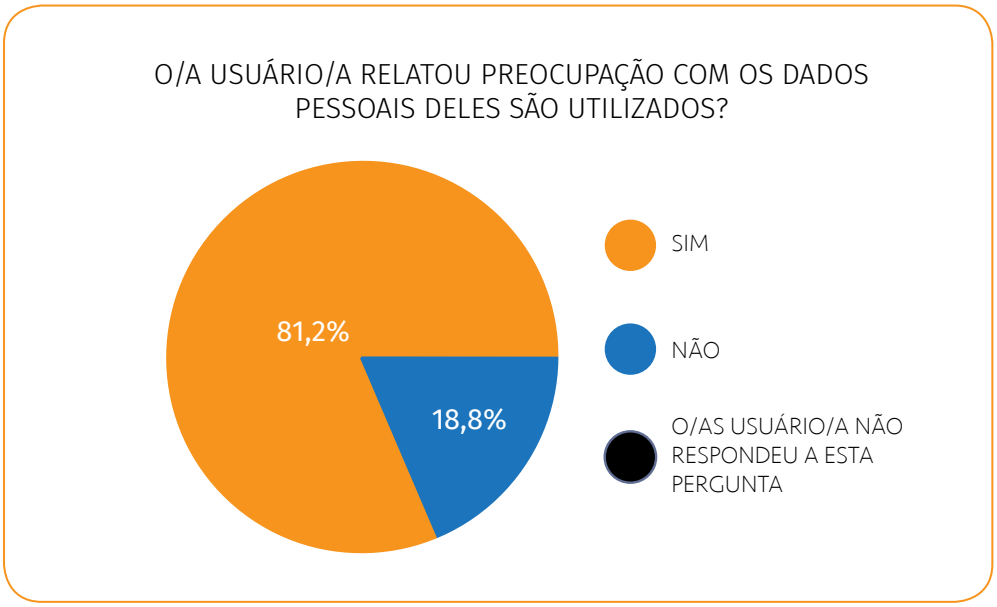
As entrevistas realizadas foram mediadas pela Associação de Diabetes Juvenil (ADJ). A seleção dessa parceria foi feita a partir das entidades representantes de usuários que convivem com doenças crônicas que compõem o Conselho Nacional de Saúde (CNS).

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 por esses pacientes. No caso da diabetes, sobretudo, considerou-se 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 maior parte dos/as entrevistados/as (10 pessoas) concentrou-se no estado de São Paulo, onde se localiza a ADJ e uma parte considerável de seus/suas associados/as. O segundo grupo (5 pessoas) está localizado em Pernambuco. E, finalmente, uma pessoa no Rio de Janeiro. Os/as usuários/as foram divididos entre usuários/as comuns, usuários/as influenciadores digitais e usuários/as que atuam na associação (ADJ).

O grupo é constituído por 43,8% de homens e 56,3% de mulheres. Com relação à faixa etária, há uma significativa heterogeneidade incluindo pessoas de 18 até 90 anos, com distribuição similar entre as diferentes faixas. Em termos de raça e renda, entre aqueles que responderam ao questionário socioeconômico (11 usuários), 63,6% declarou-se branca/o e 36,4% parda/o. Em termos de renda, 27,3% declarou possuir até 2 salários mínimos como renda familiar mensal, 9,1% de 2 a 4 salários mínimos, 45,5% de 4 a 10 salários mínimos e os demais não desejaram informar. Ressalta-se que o acesso aos usuários a partir de uma associação da sociedade civil organizada, a ADJ, influenciou o perfil de usuários entrevistados, com maioria de pessoas brancas e de classe média.

Ao serem indagados sobre se possuíam alguma preocupação com a segurança de seus dados pessoais, a maior parte (81,3%) dos entrevistados respondeu que sim, como pode ser observado no gráfico abaixo. Entretanto, ao serem especificamente indagados sobre instrumentos de consentimento com os quais estiveram de acordo, em geral não se recordam. Tampouco declararam ter uma lembrança precisa sobre o tipo de dado solicitado por serviços de saúde, farmácias, aplicativos e outros.



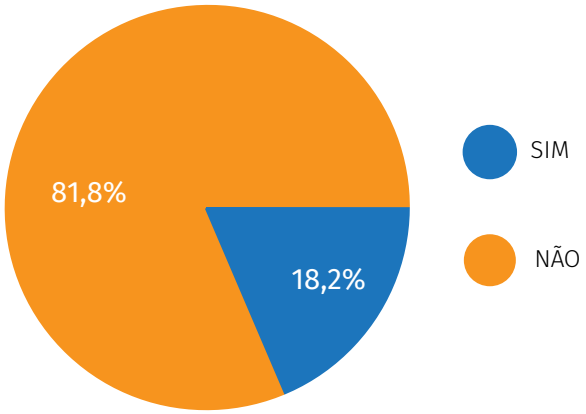
*Nós vemos os nossos dados realmente distribuídos em diversas instituições. Às vezes recebemos um e-mail em que está alguma informação nossa, sendo que nunca tivemos um acesso direto naquele local. Então isso é realmente uma questão que preocupa, essa distribuição dos dados. (Usuária, 45 anos, São Paulo-SP)*

## ENTRE OS ITENS CITADOS ENQUANTO AQUELES LEMBRADOS DE SEREM SOLICITADOS EM CADASTROS, ESTÃO:

- nome
- idade
- CPF
- número da carteirinha (convênio médico)
- impressão digital
- contato
- endereço
- e-mail
- telefone
- data de nascimento
- médico responsável
- data de quando descobriu o diagnóstico

Uma das questões feitas aos/às usuários/as foi a respeito da lembrança sobre os termos que assinaram ou concordaram e a esmagadora maioria afirmou que não se lembram.

EM ALGUM MOMENTO HOUVE UM TERMO DE CONSENTIMENTO ESPECÍFICO PARA OUSO DOS DADOS? LEMBRA DO QUE HAVIA NESTE TERMO?



A pouca lembrança sobre esse momento se liga sobretudo à urgência das demandas de saúde, a necessidade de obter um medicamento com desconto e os modelos opacos dos termos de privacidade que raramente são lidos pelas pessoas.

*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 os análogos de insulina de melhor, digamos assim, melhor resposta. Então nós nos cadastramos no programa. (Mãe de usuário adolescente, 45 anos, Recife - PE)*

**O relato acima ilustra o que a pesquisa identificou como uma tendência que é a existência da preocupação com os dados entre boa parte dos/as usuários/as, porém, na maior parte das vezes, materializar essa preocupação em formas de ação concretas que possam protegê-los/as efetivamente é difícil.** Essa dificuldade se dá, entre outras coisas, porque os/as usuários/as não conhecem exatamente o funcionamento do mercado de dados. As perguntas que questionam sobre formas de armazenamento e tratamento de seus dados, em sua ampla maioria foi respondida 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. Os usuários foram indagados sobre as formas de registro e armazenamento de seus dados e as respostas apontam para uma percepção pertinente, embora difusa e pouco assertiva:

*"Eu acho que são armazenados em servidores, o meu e de milhões de brasileiros, para pesquisa deles".*

*"Eu não consigo imaginar essa danada dessa nuvem tão grande que consegue ir tanta gente, tantos dados, mas como eu tenho um filho que faz engenharia de computação, ele me dá alguma informação dos provedores. E todos esses cadastros são feitos via provedores e a internet das coisas".*

*"Não faço ideia. Embora eu trabalhe com a área da tecnologia, só sei que fica em algum servidor. São vendidos esses dados. Isso é certeza".*

Apesar disso, os/as usuários/as foram unânimes em afirmar os benefícios que a tecnologia proporcionou para seus cuidados de saúde e a importância disso, mesmo cientes dos riscos que correm com relação à exposição de dados ao se utilizarem de tecnologias de saúde.

*Eu acho que a tecnologia tem tudo de benefício, só que eu tenho a impressão que desandou um pouco. Não tenho certeza se volta, se conseguimos fazer um retrocesso disso. Eu acho que não. É muito benéfico, você baixa o aplicativo e consegue comprar coisas muito facilmente por meio dele. Por exemplo, eu 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, 50 anos, Sao Paulo - SP)*

## PROFISSIONAIS DE SAÚDE

Os/as profissionais de saúde coletam e registram dados dos/as usuários/as dos serviços de saúde em prontuários eletrônicos e outros instrumentos. Desse grupo, interessou saber as formas de registros de exames, prescrições de medicamentos e terapias, indicações de tecnologias, e se há compartilhamento dos dados dos pacientes com outros/as profissionais e/ou serviços.

As entrevistas foram realizadas com 10 profissionais de saúde, sendo oito mulheres e dois homens, de quatro categorias diferentes: médicos (7), enfermeira (1), nutricionista (1), agente comunitária de saúde (1), que desempenham suas funções em consultórios, postos de saúde, hospital, dentre outros locais.

Em relação à rede a qual estão vinculados/as, seis atuam unicamente no Sistema Único de Saúde, um exclusivamente na rede privada e outros três trabalham no SUS e na rede privada. Dentre os/as nove que trabalham no SUS, sete são da rede municipal, um/a da rede estadual e um/a da rede federal.

**Um primeiro aspecto a destacar é o fato de que nove dentre os/as 10 profissionais entrevistados/as revelaram utilizar redes sociais ou aplicativos de mensageria para atendimento ou troca de informações com os/as pacientes, sendo o Whatsapp (sete) e o Instagram (dois) os apps mencionados.**

Uma possível explicação para o maior uso do Whatsapp é a "facilidade" de manuseio do aplicativo, ressaltada em algumas entrevistas, proporcionada pela popularização da plataforma, por sua interface intuitiva e por mecanismos como o *zero rating*[23].

Outro indicador, que aponta para a necessidade de ampliação das discussões sobre proteção de dados pessoais, é que **seis entrevistados/as afirmaram compartilhar informações de usuários com outros/as profissionais, via celular ou e-mail. Por outro lado, apenas uma entrevistada relatou saber os termos de proteção de dados das plataformas utilizadas.**

---

[23] Zero-rating, ou acesso patrocinado, é a prática de fornecer acesso à Internet sem custos financeiros sob certas condições, permitindo apenas o acesso a determinados sites ou subsidiando o serviço com publicidade.

No tocante a sistemas que coletam informações (dados pessoais) dos pacientes, nove das/os 10 entrevistadas/os afirmaram utilizar prontuários eletrônicos, sendo o PEC e-SUS[24] o mais mencionado. Prontuários privados, ainda que em menor grau, também foram citados.

**Ainda sobre sistemas de registros de dados dos pacientes no protocolo de atendimento, metade das/os entrevistadas/os informaram utilizar o Google Docs, o que reforça a preocupação com a segurança dos dados pessoais, considerando o caráter privado da empresa e, ao mesmo tempo, o desconhecimento dos/as profissionais em relação aos termos de proteção de dados.**

Além de nome completo, número do cartão do SUS e número do CPF, que foram os mais referidos, dados como endereço, telefone e nome da mãe também foram apontados pelos/as profissionais como coletados para inserção nos prontuários e outras plataformas de registro.

Chama a atenção que, dentre as/os entrevistadas/os: a) nenhum/a saiba quais tecnologias, softwares ou dispositivos são utilizados para o tratamento dos dados dos/as pacientes; b) nenhum/a saiba como as empresas e órgãos públicos tratam os dados ou mesmo se compartilham com outras empresas e instituições; c) nenhum/a tenha relatado existir medidas de segurança (técnicas ou administrativas) em relação ao tratamento de dados nos seus locais de trabalho; d) nenhum/a conhece processos de eliminação dos dados nas unidades em que atua; e) apenas duas/dois manifestaram conhecimento sobre os diferentes atores envolvidos nas etapas de tratamento desses dados; f) apenas duas/dois souberam dizer se os dados são utilizados para estudos clínicos e pesquisas, sendo, nesses casos, obrigatório o consentimento dos/as usuários (de acordo com o informado pelos/as profissionais).

Além do uso de plataformas e sistemas de coleta e registro de dados, **a telessaúde também apareceu como uma tendência crescente no trabalho dos/as profissionais entrevistados/as (cinco afirmaram já terem realizado algum atendimento mediado por tecnologias digitais, todos/as num período inferior aos últimos cinco anos), impulsionada sobretudo a partir da pandemia de Covid-19.**

Ainda que desconheçam detalhes sobre termos das plataformas e tecnologias utilizadas para coleta e registros de dados dos/as pacientes e para os serviços de telessaúde, todos/as os/as profissionais entrevistados/as entendem que há potenciais riscos ou problemas na proteção e segurança dos dados.

A percepção dos riscos e vulnerabilidades, não anula, porém, uma compreensão dos/as profissionais sobre os benefícios gerados pela coleta e registro dos dados, visto que todos/as, de alguma forma, sinalizaram ser esse uma espécie de "caminho sem volta".

## GESTORES DA REDE PÚBLICA DE SAÚDE

Enquanto responsáveis pelo gerenciamento de protocolos e fluxos de informações, os/as gestores/as dos serviços de saúde são fundamentais no processo de coleta, armazenamento e tratamento de dados dos/as usuários/as. Desse grupo, interessou-nos identificar as principais tecnologias utilizadas na coleta e tratamento de dados pessoais, quais critérios determinam ou influenciam na escolha das tecnologias e quais mecanismos de proteção de dados pessoais são adotados nas unidades de saúde.

---

[24] O PEC e-SUS é o Prontuário Eletrônico do Cidadão, software que integra as informações dos usuários do Sistema Único de Saúde, em que é possível ao profissional de saúde consultar histórico médico dos cidadãos, com acesso a informações de diagnósticos, atendimentos, exames e medicações passadas.

Foram realizadas entrevistas com 5 gestores/as, três mulheres e dois homens, todos/as da Secretaria Municipal de Saúde do Recife, sendo três médicos/as, uma fonoaudióloga e um cientista da computação, oferecendo, assim, perspectivas de diferentes áreas do conhecimento.

No que diz respeito às funções ocupadas garantiu-se também uma diversidade, contemplando-se gestores/as de regulação da média e alta complexidade; do Núcleo de Telessaúde; da Atenção Integral à Saúde; das Políticas Transversais; e da Gerência Geral de Tecnologia da Saúde.

Um primeiro aspecto verificado nas entrevistas com gestores/as foi uma visão excessivamente otimista sobre o uso de tecnologias digitais na saúde. Um indicador nesse sentido foi o uso, por todos/as os/as entrevistados/as, de expressões como "transformação digital" e "transição digital", para fazer referência ao trabalho desenvolvido pela Prefeitura do Recife. Importa enfatizar que **a perspectiva otimista no uso das tecnologias não é algo restrito a gestores/as da Prefeitura do Recife, mas uma tendência identificada em diversas áreas tanto do serviço público quanto da iniciativa privada, numa espécie de "ponto sem volta", como se as tecnologias digitais fossem a solução exclusiva para um conjunto de problemas complexos.**

*Eu acho que temos de fazer a transformação digital. Isso é inquestionável (...) Estamos investindo em tecnologia, mas sabendo que ela vem para somar, não para substituir. Nós percebemos que a tecnologia, como o agente comunitário de saúde fazendo busca ativa, a marcação de uma consulta pela regulação, é mais efetivo do que mandarmos mensagem dizendo:'a sua consulta será daqui a três dias'(GES 1).*

Também chamou a atenção nas entrevistas com gestores/as uma multiplicidade de perspectivas sobre possíveis riscos na adoção de tecnologias digitais na saúde, desde respondentes que indicam essa como uma questão de responsabilidade exclusiva da "área técnica" até outros/as que entendem a importância de fluxos mais coletivizados de discussão.

No que diz respeito aos registros de dados dos usuários, os/as gestores/as mencionaram diferentes plataformas/tecnologias, com distintos tipos de uso, a exemplo do SISREG (Sistema Nacional de Regulação), Atende em Casa e o e-SUS. **Uma questão a observar é a realização de parcerias com empresas privadas na disponibilização dessas plataformas, o que pode representar a utilização das informações por outros segmentos, repercutindo diretamente na fragilização da proteção dos dados pessoais.**

**Por outro lado, uma questão positiva constatada nas entrevistas foi o fato, de acordo com os/as gestores/as, dos dados pessoais (tanto de usuários/as quanto de profissionais) não serem compartilhados com empresas, parceiros/as e fornecedores/as, sendo a exceção apontada o uso para pesquisas, quando expressamente solicitado para esse fim.**

Demonstra-se positivo também que o armazenamento dos dados coletados esteja sob a gestão de uma empresa pública, a Emprel – Empresa Municipal de Informática, o que potencialmente possibilita uma maior fiscalização e controle públicos sobre os processos. Os/as gestores souberam informar também como e por quem os dados dos usuários são acessados/utilizados após o registro. De um modo geral, percebe-se que diferentes áreas e profissionais podem ter acesso a dados de um mesmo usuário, o que reforça a necessidade de uma política institucional de proteção dos dados pessoais.

*Os dados estão armazenados nessas bases nos datacenters e nessas nuvens. A gente consegue acessar esses dados através dos logins, ou seja, vem a base por trás. Além dos profissionais que atendem, que vê o prontuário dos pacientes que eles atendem, a gente da coordenação consegue ver como se fosse o BI que a gente pode ver, fazer a pesquisa para fazer a mentoria nessas formações, mas só pessoas das formações que têm acesso, têm essa senha. (GES 3).*

Perguntados/as sobre utilização de redes sociais e aplicativos de mensageria para atendimento ou diálogos com os pacientes, dois/as gestores/as informaram o uso do WhatsApp, sobretudo para busca de informações sobre a vacinação contra a Covid-19. Do mesmo modo, percebeu-se que há um uso recorrente do Google Docs para a gestão de informações sobre usuários e o compartilhamento dos links entre os/as gestores/as, sem que a questão da proteção dos dados seja devidamente objeto de preocupação.

Ainda sobre esse tópico, um/a gestor/a afirmou que, apesar de não haver uma normatização institucional, sabe da existência de grupos de WhatsApp criados por iniciativa de trabalhadores/as de diferentes unidades ou setores, algo que foi também apontado nas entrevistas com profissionais/as.

Como agravante, nenhum/a dos/as gestores/as informou ter promovido algum tipo de diálogo com os/as usuários/as sobre coleta e tratamento de dados nos serviços de Saúde Digital.

Também constatou-se que há diferenças de expectativas entre gestores/as e profissionais em relação ao uso das tecnologias e do próprio processo de "transformação digital" em curso pela Prefeitura do Recife, bem como a existência de orientações sobre o processo de coleta de dados pessoais sensíveis. De um lado, como dito por um dos entrevistados, "no âmbito dos gestores das unidades de serviço da média e alta complexidade, eles estão ávidos por digitalizar o processo de trabalho dos serviços". De outro, identificam-se resistências dentre os/as profissionais, sobretudo da categoria médica, de aceitação de "novas" atividades, além das já de suas rotinas. Essas resistências são motivadas por diferentes aspectos, como idade, jornada de trabalho e uma espécie de "poder social" da categoria.

## ASSOCIAÇÃO BRASILEIRA DE PLANOS DE SAÚDE E CONSELHO FEDERAL DE MEDICINA

Os gestores de empresas prestadoras de serviços de saúde e os conselhos de profissionais de saúde tiveram menor adesão e engajamento na pesquisa.

Em relação ao primeiro grupo, gestores de empresas prestadoras de serviços de saúde, o objetivo era identificar como os dados são coletados e tratados por essas empresas e se esses dados são compartilhados, permutados ou comercializados de alguma forma. No que diz respeito às representações de conselhos de profissionais de saúde, a intenção principal era compreender como esses órgãos veem a questão da proteção dos dados pessoais nos serviços de Saúde Digital e se desenvolvem ações relacionadas ao tema.

Foram realizadas duas entrevistas, uma com o Conselho Federal de Medicina (CFM) e outra com a Associação Brasileira de Planos de Saúde (Abramge). Representando a Abramge, participaram o

gerente de comunicação e a analista jurídica encarregada de proteção de dados da entidade. Do CFM, participaram três representantes, dentre os quais o encarregado de proteção de dados.

A Abramge afirmou que a proteção de dados é um tema de "bastante preocupação". Na entrevista, não foram discriminadas as medidas efetivas no tocante à proteção dos dados dos/as usuários/as, deixando isso sob a responsabilidade de cada empresa que compõe a associação. A representação da Abramge expressou visão focada na preocupação com possíveis vazamentos e não indicou pontos específicos na discussão sobre bases legais do consentimento, indicando ser esta uma responsabilidade das operadoras.

*Obviamente uma preocupação que eu acho que não é só o setor de saúde, mas uma maneira geral em todos os setores, o vazamento. A segurança e as camadas de segurança aplicáveis e como fazer isso funcionar sem travar a operação, e preservando o dado do paciente, acho que será sempre a preocupação número um das operadoras. Em termo de consentimento e base legal aplicável, eu vejo que as operadoras têm as suas próprias assessorias jurídicas, seus mapeamentos internos estão sendo realizados, seja da pequena para a grande operadora, todas de acordo com sua possibilidade financeira e sua operação, estão fazendo o dever de casa no sentido de construir tudo muito alinhado dentro da operação.*
*(Representante da Abramge)*

Já as representações do Conselho Federal de Medicina, perguntadas mais de uma vez sobre a questão da proteção de dados, forneceram respostas centradas na existência de normas regulamentares do conselho sobre a relação médico-paciente e fizeram diversas afirmações de que essas normas estão adequadas à Lei Geral de Proteção de Dados Pessoais.

.

*Então, assim, nós acreditamos (...) que as nossas resoluções, o nosso arcabouço regulamentar tem uma certa adequação razoável já com a LGPD. Ele não se baseou obviamente na Lei Geral de Proteção de Dados porque ele á anterior a ela. Nós trazemos esse tipo de interação com a lei baseado em princípios que vêm da própria Constituição. Sobretudo na questão do respeito à privacidade e à intimidade. Assim, a atividade médica em si, ela é uma atividade que envolve dados sensíveis tanto que uma das hipóteses específicas que a lei determina quanto a dados sensíveis é exatamente aquelas que envolvem a saúde do paciente.*
*(Representante do CFM)*

Uma iniciativa notável destacada pelo CFM foi a existência de dispositivos de privacidade e proteção de dados no PAE – Processo Administrativo Eletrônico, plataforma para realização de sindicâncias e processos ético-profissionais, o que tem contribuído para promover mudanças nos instrumentos de comunicação do conselho, a exemplo do site institucional.

*Então, esta plataforma por ser bem padrão do judiciário e também utilizada há muito tempo, ela já detinha nele um conjunto razoável vamos dizer assim de segurança da informação. Então, por exemplo, os atos são assinados com certificado digital ICP Brasil, todos os acessos possuem rastros de logins de acesso, então ela já dispõe de diversos recursos de segurança (...) Então, por exemplo, se você entra em um site até aquele cookie de acesso que permite você identificar a pessoa num segundo acesso e assim por diante, você precisa controlar, tem uma política de privacidade em relação a isso. Então até por isso, por exemplo, no nosso sítio, nós tivemos que remodelar e é um trabalho contínuo. Tudo é muito novo, mas há essa preocupação aqui dentro e esse trabalho nesse sentido de aperfeiçoar o sistema de informação. (Representante do CFM)*

Outro assunto abordado nas duas entrevistas foi em relação a potenciais riscos e vulnerabilidades envolvendo a proteção de dados pessoais a partir do crescente uso de plataformas digitais, sobretudo a partir da pandemia da Covid-19.

A representação do CFM explicitou a orientação geral do conselho, mas não evidenciou uma compreensão sobre a dessemelhança fundamental quando da inclusão de um dispositivo digital conectado à internet como mediador da relação médico-paciente. Em perspectiva semelhante, a Abramge falou sobre a ampliação do uso de tecnologias digitais na pandemia, mas não mencionou quaisquer riscos.

*A pandemia trouxe um boom tecnológico que estava acontecendo gradualmente e de repente virou do dia para a noite necessário e para ontem. Quem tinha um processo, seja no setor da saúde ou outro setor, com processo completamente manual, ficou para trás e teve que correr atrás do prejuízo. No setor da saúde, pela minha experiência em que eu estagiava quando tudo começou na discussão de telemedicina e tudo o mais, acredito que as primeiras mudanças foram na telemedicina, teleconsulta, como ela seria realizada, se seriam intermédicos, se seria possível uma primeira consulta já que as pessoas não poderiam sair de casa ou não deveriam sair de casa em um cenário de isolamento social, os limites para saber o que é uma emergência e quando você, enquanto médico, teria autonomia para decidir ou não manter a pessoa dentro de casa ou recorrer ao serviço de pronto atendimento, e não só na rede privada, como na rede pública também, sabemos que tiveram essas dificuldades. (Representante da Abramge)*

De um modo geral, a Abramge e o CFM demonstraram uma visão essencialmente positiva sobre os próprios trabalhos que têm desenvolvido em relação à proteção de dados, sinalizando uma aparente "falta de problemas" tanto das operadoras quanto dos profissionais médicos no tocante ao tema. As repetidas afirmações de que há uma adequação das normas regulamentares do CFM com a LGPD e com a Constituição, bem como as diversas indicações de que medidas junto às empresas de planos de saúde estão sendo adotadas, indicam nessa direção.

**Uma análise crítica das respostas, porém, evidencia que a preocupação essencial das duas entidades é possíveis vazamentos. Ou seja, com os dados já expostos e, portanto, os titulares dos dados já vulnerabilizados. A proteção prévia dos dados pessoais, relacionada com a própria noção de dignidade humana, não transpareceu como uma preocupação.**

A escuta de profissionais de saúde – não apenas de medicina – faz perceber também que há ainda um longo caminho a ser trilhado por instituições como o CFM no sentido de que a proteção de dados pessoais dos usuários esteja enraizada na cultura dos agentes do setor de saúde. Parece significativo, portanto, que essa não tenha sido uma problemática mencionada nem pelo CFM nem pela Abramge.

Após a edição da Lei Geral de Proteção de Dados Pessoais, o Conselho Federal de Medicina elaborou duas normas relativas à temática: a Instrução Normativa nº 003/2019, que regulamenta os procedimentos relativos ao acesso e ao tratamento de documentos e informações, que tem como uma das bases a Lei de Acesso à Informação; e a Instrução Normativa nº 003/2021, que estabelece a política de privacidade de dados, baseada na LGPD.

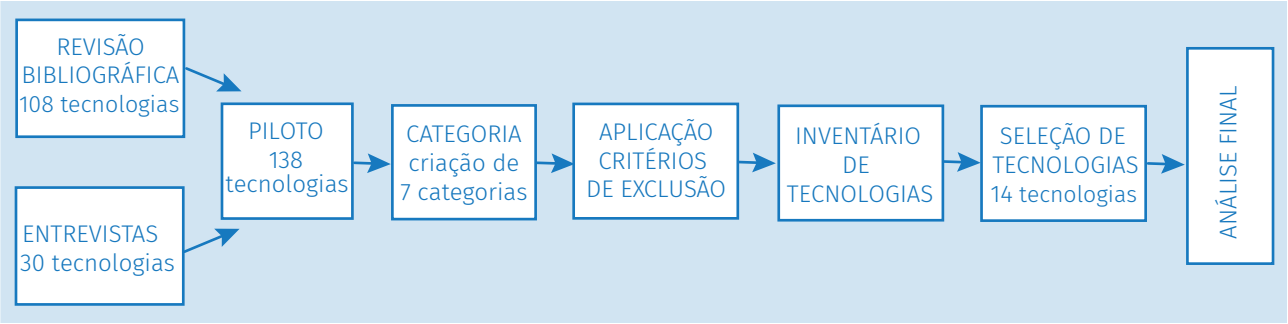
## 4.4 INVENTÁRIO DE TECNOLOGIAS DIGITAIS EM SERVIÇOS DE SAÚDE

**O Inventário de tecnologias digitais da informação e comunicação que coletam dados pessoais sensíveis em serviços de saúde** consiste em um levantamento de tecnologias digitais presentes no ecossistema de serviços de Saúde Digital no país, tanto no Sistema Único de Saúde quanto no mercado privado, com vistas a identificar as práticas de coleta, armazenamento e tratamento de dados de saúde. A partir de tal instrumento, buscou-se identificar e analisar alguns agentes presentes no ecossistema de serviços de saúde digital no país no que diz respeito à proteção de dados pessoais.

A busca por essas tecnologias foi realizada em publicações levantadas a partir da revisão bibliográfica da pesquisa, na qual foram identificadas 108 tecnologias, e das entrevistas realizadas pelo projeto, nas quais foram identificadas 30 tecnologias, totalizando 138 tecnologias inventariadas. A partir das entrevistas foi possível produzir um recorte e incluir tecnologias mais específicas, tanto territorialmente, considerando o município de Recife, como no caso daquelas voltadas especificamente para a diabetes. Após a aplicação de critérios de exclusão, a partir dos objetivos da pesquisa, chegamos a um número final de 50 tecnologias a serem categorizadas e analisadas.

## ANÁLISE DAS TECNOLOGIAS SELECIONADAS EM PRIMEIRO NÍVEL

um primeiro nível de análise foi aplicado nas 50 tecnologias inventariadas. buscou-se em primeiro lugar categorizar por tipos de tecnologia. Essa categorização foi realizada com base no texto "digital transformation in the area of health: systematic review of 45 years of evolution" (Marques, fereira, 2019). A partir de um debate realizado pelos autores, com ponderações relativas à realidade brasileira, chegou-se a sete modalidades de tecnologia para categorização do inventário, sendo que uma mesma tecnologia pode ser incluída em mais de uma categoria.




| TIPO DE TECNOLOGIA | FREQUÊNCIA |
|---|---|
| Gestão Integrada de Informação em Saúde | 18 |
| Plataformas Utilizadas para Telessaúde | 12 |
| Plataformas Utilizadas para Automonitoramento | 12 |
| Dispositivos Portáteis de Saúde | 6 |
| Sistemas de Apoio à Decisão em Saúde | 6 |
| Sistema Nacional de Informação em Saúde (SUS) | 4 |
| Redes Sociais | 2 |

Em segundo lugar, buscou-se entender dentre as tecnologia selecionadas: as suas origens (se pública, privada, parceria público-privada ou de associações da sociedade civil), os tipo de tecnologia (aplicativos, sistemas, softwares), o público a que se destina, quais as empresas desenvolvedoras e/ou proprietárias, o tipo de estabelecimento de saúde a que se destina (se hospitais, clínicas, telessaúde), o tipo de serviço oferecido/prestado, o tipo de sistema de informatização utilizado e a forma de armazenamento dos dados coletados. A seguir apresentamos as tecnologias de acordo com o público a que se destinam e a origem de suas empresas produtoras.

| TIPO DE TECNOLOGIA | USUÁRIO | PROFISSIONAL | GESTOR |
|---|---|---|---|
| Dispositivos Portáteis de Saúde | 6 | 1 | 0 |
| Gestão Integrada de Informação em Saúde | 2 | 10 | 14 |
| Sistemas de Apoio à Decisão em Saúde | 0 | 2 | 6 |
| Plataformas Utilizadas para Telessaúde | 10 | 6 | 1 |
| Plataformas Utilizadas para Automonitoramento | 12 | 3 | 1 |
| Sistema Nacional de Informação em Saúde (SUS) | 2 | 4 | 1 |
| Redes Sociais | 2 | 0 | 0 |
| Total | 32 | 26 | 23 |

Assim como a categorização dos tipos de tecnologias, a categorização que se destina a entender a que público determinada tecnologia é dirigida possibilita que uma mesma tecnologia seja destinada a públicos diferentes, algumas com a mesma interface e outras com interfaces específicas para cada público. A maior parte das tecnologias (32) é destinada a usuários/as ou tem uma interface que dialoga com esse público, seguida das destinadas a profissionais (26) e gestores (23). As tecnologias categorizadas como **Gestão Integrada de Informação em Saúde** dialogam majoritariamente com gestores (14) e profissionais (10), enquanto as **Plataformas Utilizadas para Automonitoramento** destinam-se majoritariamente a usuários (12).

| TIPO DE TECNOLOGIA X ORIGEM DA EMPRESA | Origem da Empresa | | | | |
|---|---|---|---|---|---|
| TIPO DE TECNOLOGIA | Associação Sociedade Civil | Parceria Público-Privada | Privada | Público | Total Geral |
| Dispositivos Portáteis de Saúde | | | 6 | | 6 |
| Gestão Integrada de Informação em Saúde | | 1 | 15 | 2 | 18 |
| Plataformas utilizadas para automonitoramento | 1 | | 8 | | 9 |
| Plataformas Utilizadas para Telessaúde | | 2 | 7 | | 10 |
| Redes Sociais | | | 2 | | 2 |
| Sistema Nacional de Informação em Saúde (SUS) | | | | | 4 |
| Sistemas de apoio à Decisão em Saúde | | | 1 | | 1 |
| Total Geral | 1 | 3 | 39 | 7 | 50 |

Quanto à origem das empresas, a grande maioria das tecnologias (39) é de propriedade de empresas privadas. Quando a análise segmenta o tipo de tecnologia pela origem da empresa pode-se ver que, com exceção do Sistema Nacional de Informação e Saúde, as empresas privadas lideram o desenvolvimento e a propriedade das tecnologias que fazem a mediação da Saúde Digital em todas as categorias.

A partir desse primeiro nível de análise, foram selecionadas 12 tecnologias dentre as cinquenta inventariadas para análise em profundidade. Os indicadores de análise utilizados para esse novo recorte foram elaborados a partir de critérios e parâmetros de relevância construídos com base nas análises bibliográficas e documental, nos cruzamentos feitos a partir do primeiro nível de análise e nas entrevistas. Inicialmente, a análise em profundidade seria feita em duas tecnologias de cada categoria, contudo, depois do primeiro nível de análise, percebeu-se que tanto a disparidade numérica quanto a dupla ou mesmo tripla categorização dificultaria essa aplicação e poderia gerar distorções. Optou-se, portanto, por entender a relevância das tecnologias a partir dos critérios citados acima, de forma a não incluir na análise, por exemplo, a categoria Redes Sociais, que se demonstrou menos relevante no contexto.

| NÚMERO | TECNOLOGIA | CATEGORIA | EMPRESA/INSTITUIÇÃO RESPONSÁVEL |
|---|---|---|---|
| 1 | Accu-Check Roche | Dispositivos Portáteis de Saúde | Roche |
| 2 | Bomba de Insulina Medtronic | Dispositivos Portáteis de Saúde | Medtronic |
| 3 | Conecte SUS Paciente | Gestão integrada de informação em Saúde; Plataformas utilizadas para automonitoramento; Plataformas Utilizadas para Telessaúde; Sistema Nacional de Informação em Saúde (SUS) | SUS (Ministério da Saúde - Governo Federal) |
| 4 | App Contagem de Carboidratos SBD | Plataformas utilizadas para automonitoramento | Sociedade Brasileira de Diabetes |
| 5 | App Fat Secret | Plataformas utilizadas para automonitoramento | Fat Secret/ Secret Industries Pty Ltd |
| 6 | Atende em Casa (App Recife) | Plataformas utilizadas para Telessaúde | Brayny, Pitang e Fábrica de Negócios prestando serviço para a Prefeitura do Recife |
| 7 | Conecta Recife | Plataformas utilizadas para Telessaúde | Emprel - Prefeitura de Recife |
| 8 | Google Docs | Gestão Integrada de Informação em Saúde | Google |
| 9 | WhatsApp | Plataformas utilizadas para Telessaúde | Meta |
| 10 | Prontuário Eletrônico do Cidadão (PEC) | Gestão Integrada de Informação em Saúde; Sistema Nacional de Informação em Saúde (SUS) | SUS (Ministério da Saúde - Governo Federal) |
| 11 | Memed | Gestão Integrada de Informação em Saúde MEMED | MEMED |
| 12 | Doctoralia | Plataformas utilizadas para Telessaúde | Docplanner Group |

## ANÁLISE DA CONFORMIDADE DE USO DE DADOS COM AS NORMAS LEGAIS E BOAS PRÁTICAS

A análise em profundidade das 12 tecnologias selecionadas se focou **na conformidade das práticas identificadas no uso de dados com o arcabouço normativo nacional e de boas práticas.** Dentre os critérios que foram analisados estão:

i. As bases de tratamento legal e do enquadramento dos dados nos tipos previstos na legislação (dados pessoais e dados sensíveis);

ii. O nível de proteção de dados nas coletas e tratamento de dados;

iii. O nível de conformidade com a legislação brasileira e normas mapeadas no arcabouço legal;

iv. Riscos aos dados pessoais coletados e tratados pelos agentes avaliados.

Primeiramente, cumpre destacar que **há uma falta geral de informações disponíveis sobre o tratamento de dados pessoais de maneira amigável**. A grande maioria dos produtos não se preocupa em divulgar informações referentes ao tratamento de dados de maneira complementar à política de privacidade. Apesar da grande importância e centralidade que políticas de privacidade têm como modelo, nem sempre elas são fáceis de serem consultadas a qualquer momento ou possuem linguagem acessível aos titulares de dados. Além disso, são poucas as políticas de privacidade que diferenciam o tratamento que irão realizar com dados pessoais triviais e dados pessoais sensíveis de forma evidente e esclarecida. Cerca de 60% das políticas analisadas indicam quais dados serão coletados (incluindo dados sensíveis), mas, ao versarem sobre as finalidades, tipos de tratamento a serem realizados e aplicação das bases legais (nas políticas que trazem esse tipo de informação), em nenhuma delas há distinção verdadeiramente nítida entre quando serão tratados apenas dados pessoais não sensíveis e quando serão realizados tratamentos de dados pessoais sensíveis.

**Outra informação faltante é a sobre a possibilidade de realização de inferências a partir dos dados coletados**. É sabido que essa é uma prática comum e muitas vezes necessária, mas as políticas em sua maior parte não trazem essas possibilidades, mesmo que descritas de maneira geral. Por exemplo, dados relacionados à alimentação, a depender do tratamento conferido, podem ou não ser dados sensíveis. Ainda, quando se pergunta sobre doenças crônicas, hábitos, etc., uma vez que isso é associado a uma pessoa natural, haverá tratamento de dados pessoais sensíveis.

Em relação a estruturação das políticas, alguns produtos contam com diversas políticas para descrever diferentes aspectos de sua usabilidade, seja porque há plataformas distintas para titulares que são profissionais de saúde e para aqueles que serão considerados pacientes, seja porque o uso de uma plataforma pode implicar na utilização de outra. **No entanto, poucos se preocupam em listar todas as políticas em um só lugar, de maneira organizada, e, de, na listagem, oferecer um breve resumo de cada política, dado que poucos titulares terão o tempo necessário para lê-las em sua integralidade**. Em alguns casos, os produtos nem chegam a oferecer um hyperlink para uma outra política citada no meio do texto, forçando o titular a procurá-la em sites e plataformas com os quais podem não estar familiarizados.

**Sobre informações relativas às bases legais, apesar de sua divulgação não ser uma obrigação explícita da LGPD, trata-se de uma boa prática que deveria ser seguida**. Isso porque muitos dos direitos dos titulares e da avaliação por parte do titular se os princípios da LGPD estão sendo cumpridos ou não derivam da correta escolha das bases legais. Parte das tecnologias analisadas divulgam as bases legais, mas geralmente não especificam se listam a totalidade das bases. Em muitos casos, fazem uma lista sobre quais bases de dados dos/as usuários/as usam e outra lista separada para as finalidades de tratamento, sem conectar de maneira explícita e específica uma coisa à outra.

Especificamente sobre bases legais e dados sensíveis, seria fundamental entender quais são as pessoas jurídicas de direito privado e agentes públicos que usam como base legal a prestação de serviços de saúde, pois, para isso, eles devem se considerar prestadores de serviço de saúde. **A LGPD não define o que é exatamente serviço de saúde e a ANPD tampouco se manifestou sobre isso. Mas trata-se de um tema de extrema relevância, pois ser serviço de saúde ou não pode determinar mais ou menos liberdade ou possibilidade de tratamento de dados. Entidades reguladoras de saúde também devem participar desse debate.**

**Outra questão importante a ser considerada é a de anonimização. Mesmo quando essa informação é oferecida, não são fornecidas maiores explicações ou detalhes em relação ao que se refere essa anonimização (se será referente apenas aos dados cadastrais, por exemplo)**. Conforme discutido acima, há questionamentos relevantes sobre a possibilidade de real anonimização de dados de saúde, ainda mais se tratar-se de amostras biológicas.

**Sobre o uso posterior dos dados relacionados à pesquisa, no geral, quase 70% das empresas/instituições sinalizam essa possibilidade**. Para pesquisa com dados sensíveis, no caso de entidades que não sejam órgãos de pesquisa, de acordo com a definição da LGPD, e que não possuam lei e/ou norma que autorize esse tipo de uso, usualmente elas devem coletar o consentimento do/a usuário/a ou realizar procedimentos de anonimização (uma vez anonimizados, se feito corretamente, os dados não são mais considerados dados pessoais). No caso de dados pessoais triviais, é possível invocar a hipótese do legítimo interesse. Em muitos casos, afirma-se que será realizada pesquisa apenas com dados agregados, mas não se explica se esses dados agregados incluirão também informações de saúde ou serão apenas utilizados triviais - cada caso implicará em uma base legal distinta.

**Quando se fala sobre tratamento de dados voltados para marketing, também há uma ausência de informações se serão utilizados dados sensíveis ou não para realizar esse tipo de tratamento, mesmo quando o consentimento é a base legal utilizada.**

**Ainda sobre uso secundário de dados, também se deve prestar atenção quando se trata de órgãos públicos**. Isso porque há algumas normas que autorizam, de maneira genérica, o tratamento de dados para, por exemplo, fomentar o desenvolvimento de políticas públicas. No entanto, tem-se considerado que esse tipo de autorização pode ser demasiadamente genérica e abrir porta para abusos ou para uma falta de escrutínio do poder público quanto à necessidade real de determinados dados para realizar a análise e/ou desenvolvimento de políticas públicas, ainda mais quando nos referimos a dados de saúde.

**Quanto ao compartilhamento dos dados pessoais, muitas das listadas não indicam de forma evidente eventuais terceiros com os quais possam vir a compartilhar dados ou os que lhes prestam serviços**. Por exemplo, para fornecedores de outros tipos de serviço, a divulgação nominal de quem é o parceiro é menos comum e nem sempre fica evidente quais são as medidas tomadas para viabilizar o compartilhamento (anonimização dos dados, compartilhamento de dados agregados, dentre outras medidas).

**Cerca de 60% das tecnologias analisadas, inclusive as públicas, disponibilizam explicitamente a possibilidade de integração com outras plataformas, como serviços de mensageria, redes sociais ou ferramentas da Apple e do Google (via aparelhos celulares, no caso da Apple via sistemas ioS e no caso do Google via sistemas android) que possuem aplicativos que mensuram exercício, contagem de calorias, dentre outros**.

Por um lado, a integração desses serviços os tornam mais úteis para o/a usuário/a. Por outro lado, aceitar esse tipo de integração com consciência ou configurar o compartilhamento de determinados dados ou não dependerá do conhecimento do titular sobre o que pode ser feito

com seus dados em cada instância de compartilhamento. Conforme vimos acima, apesar de haver informações disponíveis sobre o tratamento dos dados, nem sempre seu acesso é claro e geralmente há limitações na disponibilidade dessas informações. Além disso, a concentração de dados nessas grandes plataformas que dominam o mercado global contribuem ainda mais para concentrar seu poder que é baseado nos dados pessoais, com controle quase nulo por parte de usuários/as e mesmo do poder público.

**Em quase todos os casos analisados pela pesquisa, a única fonte de informação sobre tratamento dos dados é a política de privacidade, a qual possui geralmente linguagem truncada e uso de jargões jurídicos, além de poderem serem extensas. Muitas também foram simplesmente traduzidas de outros idiomas e contextos, fazendo pouco sentido na língua portuguesa e sem adequação com a legislação brasileira**. Esses foram os casos de Fat Secret, Medtronic e Accu Check, por exemplo. Dessa forma, é improvável que todos os titulares tenham todas as informações ao escolherem compartilhar seus dados ou não.

**Além disso, não fica evidente o que acontece se o usuário repentinamente decide não mais compartilhar dados ou interromper determinadas configurações nos aplicativos**. Por exemplo, caso o usuário tenha dado seu consentimento para determinado tratamento e decida retirá-lo posteriormente. Apenas Whatsapp, Fat Secret, Accu Check e Medtronic indicam tal possibilidade de forma mais clara, consistindo basicamente no encerramento da conta nos respectivos aplicativos. Algumas outras tecnologias trazem de forma vaga a possibilidade de contato por e-mail. Por mais que disponibilizar o contato do encarregado seja um requisito mínimo da lei, essa nem sempre pode ser a forma mais prática para o titular exercê-lo. Dessa forma, nesse campo, ainda falta bastante esforço das empresas que desenham as tecnologias. Essa questão se torna ainda mais complexa quando se tratam das ferramentas disponibilizadas por órgãos públicos, visto que há diversos agentes de tratamento envolvidos e, a depender do pedido, o titular deve procurar entidades diferentes.

Ainda relacionado a esse tópico, entre todas as tecnologias analisadas, somente duas - Doctoralia e Medtronic - informaram sobre o tempo de armazenamento de dados. E mesmo quando a informação aparece, é de maneira genérica ou só para alguns grupos de dados.

Outro ponto que chamou a atenção foi a questão da definição dos agentes de tratamento (ou seja, se a empresa/prestador de serviço em questão é operador ou controlador de dados pessoais). Apenas Doctoralia e Memed explicitam tal definição, porém, não explicam em detalhes como isso se aplicará ou não. Como há agentes que podem ser tanto operadoras como controladoras, a depender da finalidade do tratamento, mais informações poderiam ser dadas sobre essas diferenciações e quais seriam os papéis exercidos por esses agentes em cada etapa de tratamento, a depender do papel que ocupam. Ainda, em casos em que alguns agentes se definem como operadores, isso parece ser questionável, pois eles mesmos acabam definindo finalidades de tratamento e bases legais cruciais para o negócio, o que não seria o papel do operador, como nos dois casos citados acima.

Por fim, **quando se trata de ferramentas que serão utilizadas especialmente por profissionais de saúde para prover atendimento à população, a responsabilidade pelo uso e por informar ao cidadão sobre o tratamento parece recair quase completamente no profissional de saúde**, isso ocorre tanto no caso das tecnologias públicas como E-SUS, como no caso de outros serviços privados mediados pela interação com profissionais como o Memed. Dessa forma, muito da segurança dos dados dependerá da configuração dos dispositivos utilizados por esses profissionais de saúde, se possuem cuidado ao guardar documentos e/ou imagens, se protegem o acesso a determinados dados com senha/outros métodos de guarda de dados, dentre outras providências. Isso se salienta quando nos referimos à utilização de tecnologias que não foram desenvolvidas especificamente para a saúde, como WhatsApp e Google Drive.

Mesmo nos aplicativos desenvolvidos pelo poder público, é comum encontrar no termo avisos de que o profissional é responsável por explicar ao cidadão os pontos relacionados à sua privacidade, informando para que o dado é coletado. Ora, se isso não é colocado com clareza nas políticas, como se pode esperar que o profissional da ponta possa informar de maneira completa? Parece haver uma delegação de responsabilidade de assegurar um bom tratamento e uma excessiva responsabilização em profissionais que não possuem controle direto em relação às possibilidades da tecnologia que usam.

No caso do Google Drive, ainda seria necessário se atentar se há uma conta corporativa e se há uma instituição coordenando os acessos a determinados arquivos ou não - isso porque, se há utilização de contas pessoais, é mais difícil a gerência dos acessos, pois não se pode excluir a pessoa de um documento que ela mesma criou. Por exemplo, se um médico que atende em uma unidade de saúde, utilizando uma conta pessoal e não corporativa, insere arquivos com dados de pacientes no sistema do Google Drive e posteriormente sai daquela unidade, ele provavelmente continuará a ter acesso aos arquivos que criou por bastante tempo, mesmo que não tenha mais nenhum laço com tal serviço.

Mesmo nos casos de produtos voltados para a saúde, em muitas políticas afirma-se que, para os titulares saberem o que será feito com seus dados, devem consultar as políticas de clínicas, hospitais e serviços de saúde que contratam determinado aplicativo. No entanto, há a possibilidade dessas políticas de clínicas e serviços dependerem das funcionalidades oferecidas por esses aplicativos, se compartilham ou não determinados dados com terceiros, dentre outros fatores.

# RECOMENDAÇÕES DE ADEQUAÇÃO À LEGISLAÇÃO E BOAS PRÁTICAS

## PARA OS AGENTES QUE COLETAM E TRATAM DADOS PESSOAIS:

- Apresentar a informação sobre coleta, uso e tratamento dos dados pessoais dos/as usuários/as de forma amigável.
- "Resumir" a política de privacidade ou apresentar informações sobre tratamento de dados de forma facilitada.
- Disponibilizar informações em linguagem simples e acessível.
- Ser transparente quanto à possibilidade de realizar inferências a partir dos dados, mesmo que as inferências em si não sejam divulgadas em sua integridade.
- Quando houver diferentes formas de usabilidade listar todas as políticas em um mesmo lugar e oferecer hyperlinks para que sejam acessadas.
- Embora não seja uma obrigação explícita da LGPD, considera-se uma boa prática divulgar informações sobre as bases legais utilizadas para uso dos dados, especialmente quando há dados sensíveis envolvidos.
- Explicitar para as finalidades listadas se há diferenciação do que se aplica a dados sensíveis e a dados pessoais triviais.
- Informar sobre possíveis usos posteriores dos dados para pesquisa (mesmo quando agregados).
- Seria importante que órgãos públicos procurassem demonstrar com maior nitidez seus processos internos quanto à seleção de dados para pesquisas e seus testes de necessidade dos dados.
- Fornecer mais informações, mesmo que não seja na política de privacidade, sobre as possibilidades de marketing e quais tipos de dados são tratados para o direcionamento de anúncios e/ou outras formas de propaganda e/ou comunicação com o/a usuário/a que não tenha relação direta com a prestação do serviço.
- No caso de empresas e agentes públicos que utilizam serviços de nuvem de terceiro, é importante que indiquem qual é o provedor, já que diferentes provedores de nuvem terão especificações de seguranças distintas, de maneira que é possível ter uma ideia mais detalhada das condições de segurança.
- Explicitar como o titular dos dados poderia não mais compartilhar os seus dados e revogar seu consentimento e oferecer processos simplificados para que isso ocorra.
- Informar sobre o tempo de guarda dos dados, por quem e como.

PARA A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS:

- Que a autoridade nacional de proteção de dados, instituições de pesquisa, órgãos públicos e demais envolvidos possam discutir parâmetros eficientes para a anonimização em casos diversos.
- Que a ANPD, em diálogo com entidades reguladoras de saúde, defina de forma explícita o que é serviço de saúde, uma vez que ser serviço de saúde ou não pode determinar mais ou menos liberdade ou possibilidade de tratamento de dados.

# 5 LACUNAS REGULATÓRIAS E OS DESAFIOS PARA O DIREITO À PROTEÇÃO DE DADOS PESSOAIS EM SERVIÇOS DE SAÚDE

**O Brasil é um país com um marco regulatório atual sobre internet e proteção de dados pessoais**. O país tem, desde 2014, um Marco Civil da Internet construído a partir de um processo participativo e que é considerada uma das leis referência no setor. O país conta ainda com a Lei Geral de Proteção de Dados Pessoais (LGPD), desde 2018, e que também é considerada um avanço. No final de 2021, uma Emenda à Constituição (EC n° 115/2022) reconheceu a proteção de dados pessoais como um direito fundamental, a ser garantido pelo Estado. Estamos, portanto, diante de um país com uma legislação atual no que se refere à proteção de dados pessoais no ambiente físico e digital.

**No entanto, observam-se alguns limites e também barreiras para a incorporação de direitos digitais para a população, principalmente para a população mais vulnerabilizada cujo acesso ao ambiente digital e às tecnologias é restrito e desigual. Isso repercute no cotidiano e em diferentes esferas da vida. O abismo social do qual o digital e tecnológico fazem parte teve, no período da pandemia da Covid-19, um aprofundamento e uma complexificação ainda maior**.

A **revisão bibliográfica desta pesquisa constatou uma lacuna na literatura, sobretudo nacional, a respeito da proteção de dados na saúde em referência aos/às usuários/as e suas experiências, percepções e vulnerabilidades diante desse processo**. Apenas 8%, em um universo de 82 trabalhos analisados, ofereciam algum olhar para a presença do/a usuário/a de serviços de saúde nesse debate. Um número ainda menor de análises abordaram a percepção dos/as usuários/as sobre o tema da proteção de dados pessoais em serviços de Saúde Digital. Dessa forma, o projeto buscou enfocar os itinerários de saúde de usuários/as como ponto de partida, procurando considerar sua perspectiva no debate sobre proteção de dados pessoais.

Na observação dos itinerários de saúde, a revisão bibliográfica encontrou mais de 100 exemplos de plataformas, softwares, aplicativos e sistemas que coletam dados pessoais em serviços de saúde e que foram analisados no inventário de tecnologias.

A revisão bibliográfica indica também que vários conceitos têm sido utilizados para indicar os processos de digitalização da saúde, entre eles saúde digital, telessaúde, telemedicina, teleconsulta, associados aos conceitos de proteção de dados pessoais e privacidade, e que os diferentes usos desses termos têm implicações na prática de digitalização da saúde, o que demanda maior atenção a eles.

**Já a revisão documental das leis e normas sobre proteção de dados em saúde teve importantes achados a respeito das discussões sobre segurança**. O tratamento dado à questão da segurança costuma ser geral e superficial, colocando "segurança" como sinônimo de "cibersegurança". Também não foi observada a definição de medidas técnicas e administrativas de segurança junto às instituições e seus processos.

Nos documentos analisados foi observada ainda pouca uniformidade (ou imprecisão) na nomenclatura adotada, mesmo após a vigência da Lei Geral de Proteção de Dados (LGPD). Dentre as expressões utilizadas para "dados pessoais", por exemplo, estavam "informações pessoais", "dados do paciente" e "dados cadastrais".

Nas normas, as definições do que seria um consentimento qualificado também variam (para a LGPD, ele deve ser livre, informado e inequívoco).

Foi identificado também que as discussões sobre dados pessoais são abordadas pela lógica do sigilo (especialmente o sigilo médico). Isso parece representar uma confusão, que merece ser cuidadosamente elucidada pela pesquisa, entre privacidade (e sua ideia de liberdade negativa, de manter o Estado longe de certas esferas da vida do cidadão) e proteção de dados pessoais (e sua ideia de liberdade positiva, de permitir e até estimular o fluxo de dados, porém em um ambiente seguro e controlado).

A ausência de diálogo entre os textos das normas também foi algo que chamou atenção na revisão documental. Não foram observadas referências a outras legislações ou mesmo à LGPD na maior parte dos documentos analisados. Vale lembrar que juntar as normas esparsas sobre proteção de dados que existiam desde a década de 1990 (como o Código de Defesa do Consumidor) em um microssistema de proteção de dados era justamente o objetivo da LGPD.

**Nas entrevistas com usuários/as, observamos 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.**

**Observamos também em diferentes relatos a importância do acesso à informação. Como falar das implicações das tecnologias na saúde e da importância dos dados pessoais sem acesso à informação adequada? Como pode-se observar e conforme já era esperado, as práticas contemporâneas de acesso à informação em saúde envolvem de forma central a internet e as redes sociais.**

Como confirmam os relatos dos/as usuários/as, tais formas de interação permitem tanto uma nova forma de relação entre paciente e especialista como também entre os/as próprios/as usuários/as enquanto criadores de conteúdo. A rede social com maior centralidade citada nas entrevistas para esse tipo de acesso à informação foi, sem dúvida, o Instagram, que parece funcionar sobretudo para os/as usuários/as mais jovens como "porta de entrada" para o acesso à informação sobre saúde.

Para além das redes sociais, o WhatsApp, que é considerado um serviço de mensageria, foi muito citado como uma plataforma utilizada para telessaúde, tanto com troca de informações, mensagens e imagens, quanto para realização de videochamadas. O WhatsApp é utilizado entre usuários/as e profissionais da saúde e entre profissionais da saúde na discussão de casos clínicos.

As entrevistas indicam também que o uso de dispositivos (bombas de insulina, medidores de glicose, canetas de insulina, etc.) e insumos (insulina e medicamentos) para o tratamento da diabetes são as formas mais comuns que levam as pessoas com esse tipo de doença - e acredita-se que pessoas com doenças crônicas do geral - a se inscreverem em programas de desconto dos laboratórios ou das farmácias para compra de insumos e medicamentos com desconto.

**Sabe-se que as farmácias e os laboratórios são dois importantes pontos de coleta de dados sensíveis e que merecem ser olhados e analisados de forma cuidadosa. A pesquisa nos mostrou ainda que esses espaços se revelaram centrais na circulação dos/as usuários/as vinculando seus dados a planos de desconto de medicamentos de uso contínuo que articulam laboratórios, redes de farmácia, de supermercados e, até mesmo de roupas**.

Nesse sentido, 68,8% do total de usuários, ou 91% dos que responderam a essa pergunta, afirmaram estarem inscritos em programas de uso contínuo ou não de medicamentos de algum laboratório ou farmácia para terem desconto. A "contrapartida" oferecida pelas farmácias e pela indústria farmacêutica em troca do cadastro é muitas vezes um desconto cuja vantagem financeira se impõe muitas vezes como inegociável para a população brasileira.

Ao analisarmos as 16 entrevistas em profundidade com usuários/as pode-se observar que há, para além de uma 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 nas farmácias, por exemplo. De uma forma geral, o/a usuário/a entende que há questões não nítidas envolvidas na cada vez mais constante coleta de dados no seu cotidiano.

Chama a atenção do/a usuário/a, por exemplo, o acesso a informações, inclusive relacionadas à saúde, de empresas com as quais eles nunca compartilharam seus dados. Isso gera dúvidas sobre como essas empresas têm acesso a dados não compartilhados ou autorizados para esse fim, mas também uma sensação de impotência e de irreversibilidade da atual situação de perda de controle sobre o fluxo dos seus dados. Muitos relatos dão a entender um conformismo diante de uma situação de perda total de controle dos seus dados com a qual seria impossível "lutar contra", já que "não haveria mais" condição de reaver o controle.

A pesquisa indica que 87,5% dos/as usuários/as ouvidos/as usam dispositivos ou aplicativos relacionados à saúde e que 81,3% se preocupam com o uso dos dados pessoais, uma informação central que revela que o/a usuário/a brasileiro/a não está alheio à discussão sobre proteção de dados pessoais, mas parecem se sentir de "mãos atadas" diante de tal preocupação.

Para além da percepção do receio quanto ao compartilhamento versus a necessidade de aderir aos programas de desconto, observou-se que falta também informação e conhecimento sobre o fluxo do dado coletado (quem coleta, se e como trata, se e com quem compartilha, por exemplo), sobre os possíveis riscos do uso daqueles dados bem como a finalidade para a qual os dados são coletados. Essa ausência prática de uma informação "clara", como descreve a lei, sobre o uso dos dados dificulta uma possível equação sobre o consentimento do uso desses dados. A grande maioria, inclusive, afirmou não ler ou não lembrar do que dizem os termos de uso dos aplicativos, plataformas e dispositivos utilizados.

**Nesse sentido, como destacado no Inventário de Tecnologias Digitais da Informação e da Comunicação que coletam dados pessoais sensíveis em serviços de Saúde Digital, os serviços de saúde digitais oferecem mecanismos considerados pouco transparentes para os/as usuários/as e, sobretudo, baseados em noções de consentimento bastante frágeis tendo em vista a complexidade do mercado de dados e das interações existentes entre tecnologias, governos e grandes corporaçõe**s.

Essa realidade corrobora com o entendimento de que uma sociedade com desigualdades estruturais como a brasileira não pode ter o/a usuário/a como o principal responsável pela mitigação dos riscos associados ao compartilhamento dos seus dados. Desde a falta de uma educação que inclua o debate sobre o direito à comunicação e a proteção de dados como subsídios para uma análise de risco, passando por uma desigualdade social e pauperização da população que não garante autonomia de decisão do cidadão frente a, por exemplo, descontos na compra de um medicamento de uso crônico, chega-se finalmente a assimetria das relações entre os sujeitos envolvidos (indústria farmacêutica, grandes plataformas globais, equipamentos de saúde, redes de farmácias, etc.) e cidadãos/ãs.

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 e ao mercado indiscriminado de dados pessoais. Um rol de dados inegociáveis, a fiscalização do compartilhamento de dados sensíveis entre empresas e marcas de uma mesma empresa que atuam 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/as cidadãos/ãs em condição de garantir a proteção dos seus dados assim como acontece, ou deveria acontecer, em outros campos dos direitos fundamentais.

FIOCRUZ