Pontifícia Universidade Católica
do Rio de Janeiro

Pedro de Araújo Geraldi

Colonialismo Digital vs. Soberania de Dados: um estudo acerca do avanço das Big Techs sobre a Saúde Pública no Brasil.

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós Graduação em Análise e Gestão de Políticas Internacionais (MAPI) do Instituto de Relações Internacionais da PUC-Rio.

Orientador: Prof. Paulo Luiz Moreaux Lavigne Esteves.

Co-orientadora: Profª. Carolina de Oliveira Salgado.

Rio de Janeiro,
Agosto de 2023.

Pedro de Araújo Geraldi

Colonialismo Digital vs. Soberania de Dados: um estudo acerca do avanço das Big Techs sobre a Saúde Pública no Brasil.

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós Graduação em Análise e Gestão de Políticas Internacionais (MAPI) do Instituto de Relações Internacionais da PUC-Rio.

Prof. Paulo Luiz Moreaux Lavigne Esteves
Orientador
Departamento de Relações Internacionais - PUC-Rio

Profª. Carolina de Oliveira Salgado
Co-orientadora
Departamento de Relações Internacionais - PUC-Rio

Profª. Luiza Cruz Lobato
Departamento de Relações Internacionais - PUC-Rio

Profª. Danielle Hanna Rached
Departamento de Relações Internacionais - USP

Rio de Janeiro,
Agosto de 2023.

Pedro de Araújo Geraldi

Bacharel em Relações Internacionais pela Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio), com domínio adicional em Comércio e Negócios Internacionais, e mestrando pelo programa de Pós-Graduação em Análise e Gestão de Políticas Internacionais: Resolução de Conflitos e Cooperação para o Desenvolvimento (MAPI) da PUC-Rio.

Ficha Catalográfica

Geraldi, Pedro de Araújo

Colonialismo digital vs. soberania de dados : um estudo acerca do avanço das Big Techs sobre a saúde pública no Brasil / Pedro de Araújo Geraldi ; orientadora: Carolina de Oliveira Salgado. – 2023. 68 f. : il. color. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Instituto de Relações Internacionais, 2023. Inclui bibliografia

1. Relações Internacionais – Teses. 2. Colonialismo digital. 3. Soberania de dados. 4. Big Techs. 5. Saúde pública no Brasil. I. Salgado, Carolina de Oliveira. II. Pontifícia Universidade Católica do Rio de Janeiro. Instituto de Relações Internacionais. III. Título

COD: 327

Resumo:

Geraldi, Pedro de Araújo; Esteves, Paulo Luiz Moreaux Lavigne (orientador). **Colonialismo Digital vs. Soberania de Dados: um estudo acerca do avanço das Big Techs sobre a Saúde Pública no Brasil**, Rio de Janeiro, 2023, 68p. Dissertação de Mestrado, Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro.

O presente estudo compreende uma epistemologia crítica acerca da crescente participação de gigantes da tecnologia em setores estratégicos da administração federal no campo da saúde pública no Brasil. Primeiramente é apresentado, em ordem cronológica, o desenvolvimento das principais políticas públicas brasileiras de Saúde Digital, buscando demonstrar sua evolução e fomento à participação do capital privado na área, assim como a terceirização de serviços. Posteriormente, mobilizo os conceitos de Colonialismo Digital e Soberania de Dados para demonstrar o que a oposição entre eles representa, e como esta pode ser observada na prática, no campo da saúde. Por fim, através da análise documental e de fontes primárias, trago a pergunta de pesquisa ao estudo de caso: quais são as consequências da contratação da multinacional estrangeira Amazon - atual provedora de serviços de armazenamento e processamento de dados em nuvem para o Ministério da Saúde - para Saúde Pública no Brasil?

Palavras-chave: Colonialismo Digital; Soberania de Dados; Big Techs; Saúde Pública no Brasil.

Abstract:

Geraldi, Pedro de Araújo; Esteves, Paulo Luiz Moreaux Lavigne (orientador). **Digital Colonialism vs Data Sovereignty: a study on the advancement of Big Techs over Public Health in Brazil**, Rio de Janeiro, 2023, 68p. Dissertação de Mestrado, Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro.

This study presents a critical epistemology about the growing participation of technology giants in strategic sectors of the federal administration in the field of public health in Brazil. First, the development of the main Brazilian public policies on Digital Health is presented in chronological order, seeking to demonstrate its evolution and promotion of private capital participation in the area, as well as the outsourcing of services. Subsequently, I mobilize the concepts of Digital Colonialism and Data Sovereignty to demonstrate what the opposition between them represents, and how this can be observed in practice, in the field of health. Finally, through document analysis and primary sources, I bring the research question to the case study: what are the consequences of hiring the foreign multinational Amazon - current provider of cloud data storage and processing services for the Ministry of Health - for Public Health in Brazil?

Keywords: Digital Colonialism; Data Sovereignty; Big Techs; Public Health in Brazil.

Sumário

Lista de abreviaturas

ANPD - Autoridade Nacional de Proteção de Dados Pessoais

AppAD - Atenção Domiciliar

BNN - Base Nacional de Notificações

CDS - Coleta de Dados Simplificado

CETIC - Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação

CF - Constituição Federal

CNS - Cartão Nacional de Saúde

DATAPREV - Empresa de Tecnologia e Informações da Previdência Social

DATASUS - Departamento de informática do SUS

EACH - Escola de Artes, Ciências e Humanidades

EMBRATEL - Empresa Brasileira de Telecomunicações

ESD 28 - Estratégia de Saúde Digital Para o Brasil 2020-2028

e-SUS - SUS eletrônico

FIOCRUZ - Fundação Oswaldo Cruz

IA - Inteligência artificial

IEPS - Instituto de Estudos para Políticas de Saúde

IoT - Internet das Coisas

LGPD - Lei Geral de Proteção de Dados

MCI - Marco Civil da Internet

MS - Ministério da Saúde

OMS - Organização Mundial da Saúde

PEC - Prontuário Eletrônico do Cidadão

PNIIS - Política Nacional de Informação e Informática em Saúde

RNDS - Rede Nacional de Dados em Saúde

SD - Saúde Digital

Serpro - Serviço Federal de Processamento de Dados

SETIC - Secretaria de Tecnologia da Informação e Comunicação

SISAB - Sistema de Informação em Saúde para a Atenção Básica

SUS - Sistema Único de Saúde

SIS - Sistemas de Informação em Saúde

TSE - Tribunal Superior Eleitoral

USP - Universidade de São Paulo

É preciso aprofundar as reflexões sobre as ferramentas que fornecem e armazenam informações sobre saúde, e seus impactos – nos indivíduos e no Estado. É uma questão de soberania nacional, de defesa dos direitos e da cidadania, e da existência do SUS (MARQUES, Clarissa, 2022).

1 - Introdução

Desde 2019, os dados do Ministério da Saúde vêm sendo armazenados e processados nas nuvens de armazenamento da *Big Tech* Amazon, empresa norte-americana que, paulatinamente, vem se esforçando para adentrar o setor de saúde como provedora de análise de dados para diagnósticos, tratamentos e venda de produtos direcionados.

Frente a isso, a contratação da Amazon pelo Governo brasileiro faz parte de um processo que promove o aumento da participação do setor privado e do capital estrangeiro em áreas historicamente comandadas pelo Estado (como a área da saúde) e que, cada vez mais, vem permitindo que companhias assumam responsabilidades normalmente atribuídas a ele. Por exemplo, a gestão de ativos como dados, softwares, patentes e tecnologias, essenciais para a inovação, assim como serviços básicos como água, luz, comunicação.

Argumento que tal processo tem ampliado e aprofundado novas formas de colonialidade, isto é, uma relação hierárquica, que culmina na reprodução cotidiana de comportamentos e pensamentos que reproduzem a lógica neoliberal, como a transferência de recursos públicos para o setor privado. Resultando, assim, na manutenção dessa lógica, que favorece a destinação de recursos públicos à compra de inovações provenientes da iniciativa privada estrangeira, criando dependência de suas tecnologias, acentuando a assimetria de forças entre os países do Norte e Sul Global por meio do 'colonialismo digital'.

Deste modo, o presente trabalho desenvolve o argumento de que a externalização de serviços de tecnologia - como o armazenamento em nuvem, chave na administração pública federal brasileira - para empresas estrangeiras, torna Governo e população suscetíveis aos interesses dessas organizações e submetidos às respectivas normativas. Portanto, se apresenta como um processo extremamente preocupante, que opera para reduzir os países em desenvolvimento a territórios de extração de dados e consumidores de tecnologia externa, precisando ser debatido.

Como veremos neste estudo, a externalização escancara o colonialismo digital, podendo levar à perda de controle sobre dados críticos para a saúde pública, comprometendo a soberania nacional ao afetar a formulação de políticas públicas nesta área, bem como o desenvolvimento de tecnologias nacionais. Portanto, este trabalho se propõe ao seguinte questionamento empírico: quais são as consequências da contratação da multinacional estrangeira Amazon - atual provedora de serviços de armazenamento e processamento de dados em nuvem para o Ministério da Saúde - para Saúde Pública no Brasil?

Frente a isso, para melhor compreender o que vêm a ser o colonialismo digital, foram utilizados artigos e publicações acadêmicas desenvolvidas principalmente por Shoshana Zuboff (2019), Sérgio Amadeu (2021) e Joyce Souza (2021), que buscam discutir os impactos de um modelo de capitalismo baseado na extração de dados, assim como o avanço do setor privado na esfera pública, traçando críticas ao modelo econômico neo-liberal e apresentando as consequências desse processo. Ainda nesta temática, o podcast de Sérgio Amadeu, denominado 'Tecnopolítica', que debate, dentre diversos outros temas, os impactos das tecnologias digitais sobre a sociedade, também foi essencial para a construção desse trabalho.

No que concerne à questão da Saúde Pública no Brasil, foi dada preferência aos estudos e publicações desenvolvidos pela Fiocruz e pelo Instituto de Estudos para Políticas de Saúde (IEPS), como entrevistas, relatórios sobre Saúde Digital, e análises sobre o Complexo Econômico-Industrial da Saúde brasileiro. Também foram analisados relatórios do Ministério da Saúde, encontrados por meio da ferramenta de pesquisa Google, como por exemplo a 'Estratégia brasileira para a transformação digital (E-Digital)' e 'Estratégia de Saúde Digital para o Brasil 2020-2028', para compreender as pretensões do Ministério e como ele tem avançado nas políticas públicas de saúde.

No que diz respeito a Amazon, a fim de observar suas ambições na área da saúde e verificar dados referentes a sua participação no setor de armazenamento em nuvem, foram utilizados relatórios anuais, desenvolvidas pela própria empresa, assim como coberturas jornalísticas, nacionais e internacionais, apresentadas em portais como G1, *The Economist* e a BBC.

Para confecção deste estudo, também tive a grande oportunidade de, além da leitura de suas publicações acadêmicas, entrevistar a pesquisadora Raquel Requena Rachid, Doutoranda em Mudança Social e Participação Política pela Escola de Artes, Ciências e Humanidades (EACH) da Universidade de São Paulo (USP), que pesquisa sobre os impactos da saúde digital na Fundação Oswaldo Cruz (Fiocruz). Assim, busco aplicar um olhar crítico sobre a maneira pela qual estas tecnologias vêm sendo utilizadas e quais suas consequências para o Brasil e sua população.

O tema se mostra relevante pois é um processo ainda em curso, somado a realidade cotidiana na qual compartilhar dados e informações sensíveis se tornou pré-condição na prestação e contratação de serviços. Quem os contrata, seja um órgão governamental, empresa ou cidadão, se vê obrigado a aceitar termos de uso e compromisso, elaborados para dificultar sua compreensão e isentar as empresas de responsabilidades sobre o uso indevido desses dados por meio do consentimento. Ao mesmo tempo, a partir dessa coleta, consentida ou não,

as grandes empresas tornam-se capazes de aumentar suas receitas por meio de produtos e serviços personalizados. Como reagir neste cenário?

Deste modo, o primeiro capítulo apresenta, em ordem cronológica, o desenvolvimento das principais políticas públicas brasileiras de Saúde Digital, buscando demonstrar sua evolução e fomento à participação do capital privado estrangeiro na área, assim como a terceirização de serviços, tratando também de discutir críticas a esse movimento. Posteriormente, no segundo capítulo, mobilizo os conceitos de Colonialismo Digital e Soberania de Dados para demonstrar o que a oposição entre eles representa, e como esta pode ser observada na prática, no campo da saúde no Brasil. Também apresento exemplos de iniciativas, nacionais e internacionais, como o 'Programa de Emergência para a Soberania Digital brasileira', que têm buscado combater os efeitos nocivos do colonialismo de dados e alcançar uma independência tecnológica.

Por fim, no terceiro capítulo, é realizado um estudo empírico sobre a contratação da multinacional estrangeira Amazon como provedora de serviços de armazenamento e processamento de dados em nuvem para o Ministério da Saúde, utilizando relatórios anuais da companhia, matérias jornalísticas e explorando as tecnologias desenvolvidas por ela, para compreender seu impacto no campo da saúde. Além disso, a partir de uma metodologia indutiva, busco apresentar as consequências deste processo, que transborda do caso Amazon a outras *Big techs* que, assim como ela, procuram adentrar áreas historicamente comandadas pelo Estado, gerando uma disputa pelo conhecimento, inovação e capacidade de produzir tecnologias digitais verdadeiramente nacionais, além de comprometer a soberania nacional dos países em desenvolvimento.

2- Saúde Digital e suas implicações

2.1 - O que é Saúde Digital?

De acordo com a Organização Mundial da Saúde (OMS), a Saúde Digital (SD) diz respeito ao desenvolvimento e aplicação de tecnologias digitais, como dados de saúde, sistemas de informações de saúde, inteligência artificial (IA), *big data*, tecnologias *blockchain* e dispositivos móveis, por meio de uma abordagem multi-setorial público - privada, onde atores governamentais e não governamentais, empresas, sociedade civil, centros de pesquisa, bancos e diversos outros grupos colaboram para o desenvolvimentos de técnicas que visam aprimorar atendimentos, diagnósticos e pesquisas no campo da saúde (WHO, 2021). Buscando, inclusive, influenciar o "desenvolvimento de políticas públicas e mecanismos legislativos vinculados a uma estratégia nacional geral de saúde eletrônica" **(**WHO, 2021, p.6, tradução livre).

Portanto, a SD pode ser compreendida como a utilização de técnicas e ferramentas inteligentes para aprimorar os sistemas de saúde, promovendo a integração de diferentes campos de conhecimento para, por meio da prestação de serviços digitais, inovar, facilitar o desenvolvimento de diagnósticos, a comunicação entre diferentes níveis de atenção à saúde e romper as barreiras físicas que distanciam o paciente dos centros de atendimento (HIMSS, 2021; Ministério da Saúde, 2021). Embora a SD não seja uma novidade, ela foi popularizada devido à pandemia causada pela COVID-19, momento em que foi essencial e urgente sua aplicação devido às necessidades de se adaptar às medidas de segurança estipuladas pela OMS, com ênfase no distanciamento social.

2.2 - O Sistema Único de Saúde (SUS)

Inaugurada por meio da Constituição Brasileira de 5 de outubro de 1988, a política de Saúde Pública do Brasil buscou estabelecer que "a saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário (...)" (CRF do BRASIL, 1988). Com isso, propondo alcançar este objetivo, foi desenvolvido o Sistema Único de Saúde (SUS), oficializado pelas leis 8.080/1990 e 8.142/1990. Reconhecido como maior sistema público de saúde do mundo, busca proporcionar o acesso universal à saúde – ou seja, que todos os cidadãos brasileiros tenham direito aos serviços de saúde, sem discriminação (FIOCRUZ,

2023b) – para promover uma melhor qualidade de vida à população, incluindo medidas para melhora e extensão do atendimento médico, além do estímulo à vigilância sanitária, saúde e pesquisa (Ministério da Saúde, 2011).

Inicialmente, conforme observado por Scheffer e Souza (2022), por meio da Lei Orgânica da Saúde – lei nº 8.080, de 19 de setembro de 1990 –, em seu artigo n° 23, buscou-se restringir a participação do capital estrangeiro no SUS, conforme lê-se:

> É vedada a participação direta ou indireta de empresas ou de capitais estrangeiros na assistência à saúde, salvo através de doações de organismos internacionais vinculados à Organização das Nações Unidas, de entidades de cooperação técnica e de financiamento e empréstimos (BRASIL, 1990).

Porém, sob justificativa de tornar mais eficientes os serviços oferecidos, de maneira gradual, por meio de marcos regulatórios e licitações, foram permitidos investimentos estrangeiros em áreas como assistência médica suplementar, planos e seguros de saúde, até que, em 2015, o setor foi aberto ao capital estrangeiro (SCHEFFER e SOUZA, 2022, p.2). Esta ampla, porém gradual abertura ao mercado, somada a diversas estratégias para modernizar e aprimorar os atendimentos na área, pode nos ajudar a compreender o que vem a ser o processo de fomento à 'plataformização' no SUS (RACHID et al, 2022) – conceito esse que será melhor desenvolvido à frente – em paralelo ao que hoje é conhecido como saúde digital no Brasil. A SD foi particularmente desenvolvida a partir da portaria n°589/2015, onde o Ministério da Saúde (MS) instituiu uma nova versão da Política Nacional de Informação e Informática em Saúde (PNIIS) – política que estabelece as principais diretrizes para utilização e adequação das tecnologia da informação e comunicação no sistema de saúde brasileiro – que, somada a sua evolução a de diversas outras políticas, apresentadas abaixo, serviram de base para a 'Estratégia de Saúde Digital Para o Brasil 2020-2028' (ESD 28).

2.3 - Principais políticas brasileiras de fomento a SD

Em 1991, o Departamento de Informática do SUS (Datasus) foi criado, absorvendo a responsabilidade de controle e processamento das informações e dados da população brasileira referentes ao setor de saúde, que até então pertencia a Empresa de Tecnologia e Informações da Previdência Social (Dataprev) (Ministério da Saúde, 2002). Agora, sob responsabilidade do Ministério da Saúde, observava-se "a importância da informação para os processos de gestão e formulação de políticas", além da utilização da internet e recursos tecnológicos para comunicação e gerenciamento de operações em âmbito nacional (Ministério da Saúde, 2002). Dentre as competências que, por decreto, ficaram definidas para o Datasus,

além da definição de normas e padrões a serem seguidos, é possível observar o desejo de fomentar e avaliar o desenvolvimento de pesquisas para implementação e aplicação de tecnologias voltadas a informatização do SUS; também, a necessidade de criação e manutenção de uma base de dados de saúde unificada de toda a população brasileira (Ministério da Saúde, 2002). Representando, assim, os primeiros passos do Governo para promover a utilização de recursos tecnológicos para estruturação de um repositório de informações em saúde de capilaridade nacional, buscando o desenvolvimento de políticas públicas mais embasadas nos dados pessoais e sensíveis da população. Por dados sensíveis, caracterizam-se aqueles

> referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

Cerca de onze anos depois, em 2012, frente aos avanços das tecnologias da informação em âmbito global, assim como o acesso mais amplo à internet e redes móveis, o MS iniciou o projeto de um SUS eletrônico (e-SUS), aplicando o conceito de e-saúde – "uma estratégia para a adoção de padrões de informática em saúde para o atendimento de diretrizes propostas pelas políticas de informação em saúde mundiais" (Ministério da Saúde, 2016). Por meio de um modelo mais atualizado de gestão de informações, o e-SUS visa otimizar a coleta de dados sensíveis da população brasileira, possibilitando a individualização dos pacientes e integração com outros sistemas da atenção básica, como por exemplo o CDS (Coleta de Dados Simplificado), o PEC (Prontuário Eletrônico do Cidadão) e o appAD (Atenção Domiciliar), e do SUS (Ministério da Saúde, 2016).

Não obstante, no que diz respeito ao contexto regulatório, este projeto faz com que o MS substitua a primeira proposta da Política Nacional de Informação e Informática em Saúde (PNIIS), publicada em 2004, por uma nova versão, incorporando o conceito de saúde digital (RACHID et al, 2023), sendo essa a primeira atualização da PNIIS. Com isso, em 2015, visto a crescente necessidade de uma política que guiasse a maneira pela qual as tecnologias da informação são utilizadas no SUS, além de desenvolver uma estratégia para nortear o tratamento dos dados de saúde em âmbito nacional e estimular a participação dos centros de pesquisa, foi instituída, por meio da portaria nº 589, a versão atualizada da Política Nacional de Informação e Informática em Saúde (Ministério da Saúde, 2016).

Com isso, a PNIIS 2.0 expande suas orientações para incluir soluções digitais na área da saúde, com ênfase no uso de recursos tecnológicos, tais como prontuários eletrônicos e

aplicativos para atendimentos à distância; além disso, busca estabelecer o compromisso de profissionais e estabelecimentos de saúde, tanto públicos quanto privados, em fornecer dados para o DATASUS, assim como responsabilidade sobre o uso adequado dos dados de saúde (MARINHO, 2020). Neste caso, podemos compreender como uso adequado aquele que busca não prejudicar os usuários, evitando práticas discriminatórias e desrespeitosas, de maneira a garantir que as informações que estão sendo alimentadas no sistema respeitem os princípios de universalização do SUS, também os interesses de quem os está fornecendo. Logo, a PNIIS 2.0 buscou apresentar-se como uma política norteadora, visando a melhor governança do uso dos dados sensíveis da população brasileira, além de enfatizar o "poder transformador da tecnologia da informação a fim de melhorar os processos de trabalho em saúde e resultar em um Sistema Nacional de Informação em Saúde" (Ministério da Saúde, 2016, p.11).

Ainda em 2015, por meio da Lei n°13.097/2015, alterou-se a Lei Orgânica da Saúde – Lei nº 8.080/1990 – de maneira a fortalecer a abertura à participação do setor privado, do capital estrangeiro, e às terceirizações na oferta de serviços de saúde. Vale ressaltar que essa alteração ocorreu em um período de instabilidade no Brasil, que presenciava crises políticas e econômicas. Neste mesmo ano, a economia brasileira observou um recuo de 3,8% em relação ao período anterior, somado a uma taxa de desemprego de 8,1% e déficit público de 10,38% – quando os custos do governo superam sua receita –, apresentando deterioração fiscal (NETO, 2016).

Conforme demonstrado por Scheffer e Souza (2022), o impacto desta alteração foi direto, posto que no período de 2016 a 2020, com a abertura promovida pela alteração, o valor de investimentos em saúde no Brasil atingiu a marca de USD 348 milhões, representando um aumento de quase dez vezes em relação aos anos cinco anos anteriores. Além disso,

> houve expansão de conglomerados econômicos da saúde, caracterizando novos laços societários entre grupos (...). Há sinais de maior concentração de investimentos domésticos entre planos de saúde, hospitais, clínicas e laboratórios de diagnóstico. Grandes grupos passaram a promover fusões entre si ou adquiriram empresas menores, visando expansão territorial, ganho de escala em operações e verticalização da rede assistencial (SCHEFFER e SOUZA, 2022 , p. 8 - 10).

Por exemplo, de acordo com a Fiocruz (2020), em 2020, as três maiores empresas de serviços de saúde no Brasil eram: Amil, com patrimônio líquido de R$ 12 Milhões; Hapvida, com R$ 07 milhões; e NotreDame Intermédica, com R$ 06 milhões. Somado a isso, cabe mencionar que a Amil foi comprada pelo grupo Norte-Americano *UnitedHealth* em 2012, e as empresas Hapvida e NotreDame Intermédica, que pouco depois vieram a se tornar uma só

empresa, foram compradas pelo fundo Norte-Americano *Bain Capital* em 2014 (Fiocruz, 2020; Globo, 2017).

Portanto, observa-se que a intensificação da abertura do setor de saúde para investimentos privados estrangeiros ocorreu em um momento de crises políticas e econômicas no país, e o resultado foi a concentração de mercado em poucas empresas, dando a estas maiores possibilidades de barganha e poder político, haja vista sua predominância. Assim, o enfraquecimento do Complexo Econômico-Industrial da Saúde brasileiro se apresenta como consequência dessa internacionalização, posto que teve reduzida sua capacidade de utilizar as instalações de saúde como um meio para fomentar o desenvolvimento produtivo, científico e tecnológico nacionais.

Pouco depois, em 2017, a partir do desenvolvimento da PNIIS 2.0, foi elaborada a "Estratégia e-Saúde para o Brasil" que, por sua vez, busca inspiração em experiências realizadas em outras áreas, como a bancária, para apresentar uma maior participação do setor privado na concretização das políticas públicas de saúde, "integrando programas e agregando recursos de todos os setores das três esferas de governo, da sociedade civil e da iniciativa privada" (Ministério da Saúde, 2017, p.12). Aqui destaca-se, além de definir e implementar os sistemas e serviços de e-Saúde integrados ao SUS, a iniciativa de elaborar um marco legal, proporcionando um processo mais transparente e um arcabouço legal para o desenvolvimento da SD (Ministério da Saúde, 2017).

Vale ressaltar que, neste momento, ainda não estava consolidada a Lei Geral de Proteção de Dados (LGPD), lei que define diretrizes para a proteção da privacidade e dos dados pessoais, incluindo dados de saúde, durante a coleta, armazenamento, processamento e compartilhamento dessas informações (BRASIL, 2018), promulgada em 2018 e implementada somente em 2020. Por este motivo, uma terceira versão da PNIIS foi elaborada em 2021 para se adequar a LGPD, de maneira a garantir o direito do cidadão a maior autonomia e acesso aos dados e informações de saúde, assim como a manutenção da integridade e rastreabilidade desses dados; além disso, visa proibir que essas informações sejam utilizadas de maneira indevida por empresas e operadoras de planos de saúde privados (ANTUNES, 2021; SAMARCO, 2021).

Isto posto, a intenção de garantir maior segurança sobre o tratamento dos dados sensíveis dos cidadãos brasileiros fica clara nos seguintes pontos, presentes no "Capítulo 01 - Disposições gerais", do texto da PNIIS 3.0:

> VI - preservação da autenticidade, da integridade, rastreabilidade e da qualidade da informação em saúde, observado o disposto na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados;

> VII - confidencialidade, privacidade, proteção de dados e segurança da informação de saúde pessoal como direito de todo indivíduo;
> VIII - autonomia do usuário na decisão sobre o compartilhamento dos seus dados de saúde com profissionais da área de saúde que atuem na sua assistência, com órgãos de pesquisa ou com órgãos ou entidades de saúde públicas e privadas, respeitadas as obrigações legais de compartilhamento para vigilância em saúde e gestão da saúde pública; (BRASIL, 2021).

Portanto, além de se posicionar em concordância com a LGPD, dando destaque a segurança da informação de saúde pessoal como direito de todo indivíduo, a terceira versão da PNIIS também busca promover a maior autonomia do usuário sobre o compartilhamento de suas informações sensíveis, enfatizando a importância do consentimento nas relações entre paciente e profissional de saúde, tanto na rede pública quanto privada.

Inclusive, conforme apontado por Samarco (2021), a PNIIS agora reconhece a utilização de novas ferramentas, dotadas de inteligência artificial, *big data* e dispositivos inteligentes, para melhoraria dos processos de saúde e maior embasamento das políticas e pesquisas no campo (SAMARCO, 2021), podendo ser observado na seção VI[1] - "Ambiente de conectividade em saúde" do novo texto do documento. Porém, pouco é discutido sobre como os dados recolhidos pelos SUS serão protegidos em relação ao setor privado, fragilizando-os (PINTO, 2022 apud PASSOS, 2022).

Consequentemente, levanta dúvidas sobre como estas informações serão utilizadas. Posto que, embora a terceira versão da PNIIS se proponha a garantir maior segurança às informações de saúde e dados pessoais dos usuários, ao reconhecer a utilização de IA e *big data,* ferramentas geralmente desenvolvidas e geridas por empresas estrangeiras, para melhoria dos processos de saúde, ao não discutir como os dados recolhidos pelos SUS serão protegidos em relação ao setor privado, acaba por priorizar a inovação e a produtividade em detrimento da proteção de dados. Ainda, apenas cita que o cidadão terá mais autonomia neste compartilhamento, sem especificar quando será necessário seu consentimento.

Pouco depois, ao longo do período de 2019 - 2020, foi publicado o "Plano de Ação, Monitoramento e Avaliação da Estratégia de Saúde Digital para o Brasil 2019-2023", buscando apresentar uma direção para sua consolidação. Com isso, ao avaliar a estrutura de governança – como a capacidade de ação estatal na implementação das políticas desejadas – o Plano visa estabelecer objetivos considerados viáveis para promoção da SD (Ministério da Saúde, 2020). Neste Plano, destaca-se a iniciativa de desenvolvimento do Conecte SUS –

[1] Neste documento, seção VI, artigo 9° lê-se: "III - uso de big data em saúde, para fornecer evidências para políticas, pesquisa e planejamento para que as descobertas na saúde digital se traduzam em ações;
IV - promoção da disseminação de dados e informações em saúde e do uso de inteligência artificial de forma a atender tanto às necessidades de usuários, de profissionais, de gestores, de prestadores de serviços e do controle social, quanto às necessidades de intercâmbio com instituições de formação, ensino e pesquisa, entre outras;".

“programa voltado à informatização da atenção à saúde e à integração dos estabelecimentos de saúde públicos e privados e dos órgãos de gestão em saúde dos entes federativos” – por meio da implementação de uma Rede Nacional de Dados em Saúde (RNDS), além da intenção de aquisição de nuvem para armazenamento dos dados sensíveis coletados (Ministério da Saúde, op. cit).

Ainda, o Plano se relaciona com a PNIIS 3.0 na medida em que, reconhecida a sensibilidade no tratamento dos dados de saúde, apresenta como prioritário a adequação às exigências propostas pela LGPD, de maneira a garantir a confidencialidade, privacidade e proteção dos dados sensíveis (Ministério da Saúde, op. cit). Para que assim seja possível implementar, de maneira sólida, a SD no Brasil. Não obstante, reconhece que a SD estará em permanente construção e, portanto, o Plano, que abrange o período de 2019-2023, configura-se como o primeiro de outros que virão, de maneira cíclica, buscando monitorar e avaliar as estratégias de SD que vêm sendo desenvolvidas. Com isso, haja vista sua implementação, definida como um processo de longo prazo, em etapas, temos que o primeiro passo estipulado pelo documento foi justamente a implementação da RNDS, promovendo a integração nacional e “a troca de informações entre os pontos da Rede de Atenção à Saúde (RAS), permitindo a transição e continuidade do cuidado nos setores público e privado” (Ministério da Saúde, op. cit, p.14).

A RNDS, instituída pelo MS em 2020, tem como objetivo centralizar o armazenamento dos dados de saúde da população brasileira, proporcionando a troca de informações, por meio de diferentes aplicações, entre os setores público e privado, dentre os diferentes níveis de atenção à saúde, de maneira a desenvolver uma plataforma única nacional de saúde (Ministério da Saúde, op. cit). O Conecte SUS, por sua vez, é uma plataforma digital, materializada em aplicativo, que busca permitir que seus usuários possam acessar históricos de exames, vacinas, medicamentos, internações etc, informações estas armazenadas pela RNDS, e compartilhá-las com diferentes estabelecimentos de saúde, públicos e privados, de maneira a reduzir os esforços da coleta de informações e otimizar os atendimentos de saúde (Ministério da Saúde, op.cit).

O aplicativo logra êxito na sua função de otimizar a vida do usuário, facilitando consultar seu percurso nos mais diferentes serviços dos SUS. Ademais, é possível aferir que, durante a pandemia da Covid-19, foi essencial para a manutenção dos mais diversos estabelecimentos comerciais, a exemplo dos restaurantes e cinemas que, buscando manter seus serviços e ao mesmo tempo impedir o aumento das taxas de contágio, solicitaram ao

público seu histórico de vacinação, informações essas com acesso facilitado pelo Conecte SUS.

Figura 01: Ações disponibilizadas pelo aplicativo Conecte SUS.

Fonte: aplicativo Conecte SUS (2023).

Por fim, no período de 2020 - 2021, temos a publicação da "Estratégia de Saúde Digital Para o Brasil 2020-2028 (ESD 28)", com objetivo de materializar e expandir a proposta de e-saúde, em especial a consolidação do Conecte SUS e da RNDS (Ministério da Saúde, op. cit). Diferente de suas antecessoras, esta nova Estratégia apresenta a intenção de desenvolver o que denominam de 'ecossistema compartilhado de inovação', também proposto na última versão da PNIIS, de maneira a convidar empresas de tecnologia – *Big Techs* – que desenvolvem ferramentas de *Big Data* e Internet das Coisas (IoT) para utilizar a RNDS como laboratório para descoberta de novas tecnologias voltadas à saúde, além de compartilhar conhecimentos entre si, visando o desenvolvimento de novas iniciativas que possam melhorar atendimentos e diagnósticos (Ministério da Saúde, op. cit).

De todo modo, vale ressaltar que, infelizmente, nesta Estratégia pouco é apresentado sobre como fomentar o desenvolvimento de tecnologias brasileiras no campo, assim como

avançar em pesquisa local sobre mecanismos de inteligência artificial. Nela, prioriza-se a terceirização de serviços, o que acaba por aumentar a dependência de inovações que vêm do exterior e, ao mesmo tempo, torna os cidadãos mais vulneráveis, posto que seus dados são compartilhados sem total garantia de segurança cibernética. Além disso, esbarra em obstáculos, como as desigualdades socioeconômicas relacionadas ao acesso à internet, que dificultam o acesso às ferramentas e tecnologias necessárias para utilizar as inovações apresentadas pela ESD 28, como os atendimentos a distância (DIÓGENES e RIBEIRO, 2023).

Exemplo claro destas desigualdades foi relatado pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC) (2021), que observou que a ampliação do uso de tecnologias de informação e comunicação no setor da saúde também evidenciaram o impacto da exclusão digital ao agravar disparidades sociais e econômicas, incidindo, especialmente, sobre a parcela mais carente da população brasileira, sem acesso à internet ou com conexão limitada. De acordo com estudo realizado, a prática do atendimento à distância, entre 2021 e 2022, foi mais utilizada por aqueles com maior poder econômico, pertencentes às classes 'A e B', representando 42% do total de consultas online, seguida pela classe 'C', com 22% , e 'D e E', com 20% (CETIC, 2021b apud ALMEIDA, 2023). Além disso, o CETIC também analisou onde os usuários procuravam estes atendimentos, nas redes públicas ou privadas: de acordo com a pesquisa, 82% dos usuários das classes A e B buscaram a rede privada para suas consultas virtuais, enquanto 78% dos usuários das classes D e E recorreram à rede pública (CETIC, 2021b). De igual modo, "esse serviço esteve mais presente nos estabelecimentos privados (22%), nos localizados na região Centro-Oeste (24%) e nos sem internação (21%)" (CETIC, 2021b, p.80).

Portanto, cabe a reflexão: tendo em vista a falta de fomento ao desenvolvimento de tecnologias locais, somado às desigualdades econômicas que apresentam obstáculos à universalização dos serviços digitais, será essa a melhor estratégia para atender às demandas de saúde da população brasileira? Quais interesses estão em primeiro lugar: os da população ou da iniciativa privada? Logo, com a falta de investimento em tecnologias locais, temos que, por exemplo, os interesses externos são priorizados no desenvolvimento de medicamentos e vacinas em detrimento da manufatura local. Nesta toada, o Brasil se mantém dependente da produção farmacêutica de outros países e de insumos estrangeiros, colocando-se em situação de subalterno, o que acaba por afetar diretamente o acesso da população a medicamentos no país (MARCHIORI, 2022). Assim,

> é cada vez mais importante que nós façamos uma reflexão sobre a necessidade do investimento nacional nas pesquisas e na indústria, nos laboratórios nacionais e nas universidades, no sentido de que possamos trabalhar em medicamentos para as nossas necessidades e que não fiquemos na dependência de fatores externos, sobre os quais nós temos poucas possibilidades de interferir (SANTOS, 2022 apud Marchiori, 2022, p.1).

Na Tabela 1, abaixo, temos um resumo das principais políticas de fomento à SD no Brasil que foram apresentadas até aqui.

Tabela 01: Principais políticas de fomento à Saúde Digital no Brasil entre 1991-2021

Período	Resolução ou documento norteador	Resultado
1991	Decreto nª100, de 16 de abril de 1991	Datasus
2009	Portaria nº2.690, de 05 de novembro de 2009	Política Nacional de Gestão de Tecnologias em Saúde
2012/13	Portaria nº 1.412, de 10 de julho de 2013	e-SUS
2015	Portaria nº 589, de 20 de maio de 2015	PNIIS
2016	Decreto nº 8638, de 15 de janeiro de 2016	Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional
2016	Resolução nº5, de 25 de agosto de 2016	Comitê Gestor da Estratégia e-Saúde
2017	Resolução nº 19, de 22 de junho de 2017	Estratégia e-Saúde para o Brasil
2019	Decreto 13.787, de 27 de dezembro de 2018	Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente
2019	Portaria Ministério da Saúde nº 676, de 17 de julho de 2019	Plano Diretor de Tecnologia da Informação e Comunicação 2019-2021 (PDTIC)
2019	Portaria nº 2.983, de 11 de novembro de 2019	Informatiza APS - Programa de Apoio à Informatização e Qualificação dos Dados da Atenção Primária à Saúde
2019	Ad Referendum na CIT, em 30 de março de 2020	Plano de Ação, Monitoramento e Avaliação da Estratégia de Saúde Digital para o Brasil 2019-2023
2020	Portaria nº 1.434, de 28 de maio de 2020	Rede Nacional de Dados em Saúde - RNDS

2020	Portaria nº 1.434, de 28 de maio de 2020	Conecte SUS
2020	Portaria nº 3.632, de 21 de dezembro de 2020	Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD 28)
2021	Portaria nº 1.768, de 30 de julho de 2021	Nova versão da Política Nacional de Informação e Informática em Saúde

Fonte: Elaboração própria.

2.4 - Críticas ao processo de abertura da saúde à iniciativa privada estrangeira

Embora sob a justificativa de tornar mais eficientes os serviços de saúde brasileiros mediante maior participação da esfera privada, buscando incentivar inovações tecnológicas, investimentos e fomentar o intercâmbio de conhecimento, a abertura da saúde exposta acima precisa ser analisada com olhar crítico. Conforme observado por Rachid (2022) em entrevista disponibilizada pela Fiocruz, compreende-se que a digitalização de tais serviços provoca um movimento de potencial destinação de recursos públicos à iniciativa privada, visto que as estratégias brasileiras de SD representam o avanço do capital estrangeiro sobre a área da saúde.

Este avanço, por sua vez, pode ser explicado pelos próprios interesses mercadológicos dessas empresas que, buscando constantemente aumentar suas receitas, expandindo sua cartela de clientes e os serviços a eles prestados, encontram no Brasil uma base extremamente atrativa, com cerca de duzentos milhões potenciais "consumidores". Dentre esses interesses, também se encontra a perversa intenção de reduzir a saúde a um serviço, e não mais um direito, haja vista a constante busca por lucro.

Concomitantemente, tem-se que os investimentos governamentais na área encontram-se estagnados ou foram reduzidos ao longo dos anos, onde

> Entre 2013 e 2023, a participação do investimento na saúde recuou em 6 pontos percentuais. Em valores absolutos, a dotação atual, de R$ 6 bilhões, é 64,2% menor que a da década passada, R$ 16,8 bilhões, e a sua alocação é cada vez mais determinada por emendas parlamentares (FARIA e NOBRE, 2023, p.1).

Essa estagnação pode ser compreendida, em parte, como resultado do atual modelo econômico vigente, neo-liberal, que favorece a destinação de recursos públicos à compra de inovações provenientes da iniciativa privada, soluções essas que acabam sendo menos custosas a curto prazo, ao invés de promover o desenvolvimento nacional.

Logo, quais são os riscos dessa abertura da saúde à iniciativa privada? Em síntese, temos: (i) o enfraquecimento do SUS, visto que acarreta em transferências de bens públicos (recursos humanos e financeiros) para o setor privado; (ii) a abertura a negociações e contratos que atendam aos interesses privados, e não os da população, em especial a parcela mais vulnerável; (iii) o aprofundamento da austeridade e do sub-financiamento já presentes na área; (iv) o enfraquecimento da força de organização social dos profissionais da saúde – que observam, por exemplo, o aumento de contratos temporários e a corrosão de direitos trabalhistas – e; (v) a ameaça ao papel do Estado como garantidor dos direitos relacionados à saúde, conforme previsto na CF de 1988 – ao passo que o caráter complementar da iniciativa privada vem se transformando, isso implica na retirada do setor público e predominância do setor privado na prestação de serviços de saúde (CEGATTI et al, 2020). Isto pois

> as falhas no processo de regulação do setor privado sugerem uma crescente e descontrolada participação deste setor na saúde, e, com isso, passa a possuir expressivo poder político e de pressão no que se refere a negociação e intermediação de seus contratos, bem como a remuneração de serviços prestados (ROMANO e SCATENA, 2014, apud CEGATTI, 2020, p26).

Outro ponto importante, conforme alertado por Rachid (2022), é perceber que o Brasil tem presenciado diversas iniciativas tecnológicas – como os aplicativos para monitoramento de saúde e atendimentos à distância – inspiradas e desenvolvidas pela iniciativa privada, que visam solucionar as falhas do SUS. Falhas essas, por exemplo, como a sobrecarga dos centros públicos de atendimento, que frequentemente operam no limite de suas capacidades humanas e financeiras. Buscando, por meio da maior participação privada e a introdução de um modelo de negócios, atrair acionistas, aliviando a carga do setor ao melhorar os serviços prestados e o atendimento dos pacientes de maneira geral.

Porém, essas iniciativas são embasadas em um discurso que traz forte influência do mundo corporativo, especialmente no que se refere às estratégias de digitalização da saúde pública, onde tem-se buscado vincular sua abertura a mercados tecnológicos rentáveis – como o mercado de desenvolvimento de aplicativos e assistentes virtuais – apresentando-se como a resposta para as dificuldades enfrentadas pelo SUS na garantia de uma saúde universal (RACHID, 2022).

Fomentando, inclusive, o que a pesquisadora define como processo de ‘plataformização’ do Estado - este movimento de digitalização dos serviços prestados pelo Estado, de maneira a atender principalmente às demandas da indústria de tecnologia por meio da criação de um mercado consumidor (RACHID, 2022). Assim, baseada na iniciativa privada, em especial do exterior, e no desenvolvimento da Internet das Coisas (IoT) –

tecnologias que permitem a troca de dados por redes conectadas – sustenta-se a lógica de geração de valor por meio da privatização de infraestruturas públicas, criação e manutenção de cidadãos-consumidores de serviços assistenciais de saúde e, principalmente, fomenta a coleta massiva de dados da população, essencial para o funcionamento dos serviços digitais (RACHID, 2022). Com isso, o "SUS torna-se um grande mercado consumidor de soluções pré concebidas pelo setor privado e sem resolutividade comprovada, que minam a soberania nacional em relação aos dados de saúde da população brasileira" (MORAES, Ilara, 2022, p.7).

Portanto, a maior participação do mundo corporativo, principalmente a iniciativa privada estrangeira, que não prioriza nem desenvolve os princípios básicos do SUS de universalização e equidade, apresentam-se como possível risco à saúde pública brasileira. Assim, este processo vem caminhando para reduzir a saúde a um serviço, e não mais um direito da população, tornando-se mais um obstáculo para SUS.

2.5 - O que são Nuvens Públicas e o curioso processo de terceirização desses serviços a empresas privadas estrangeiras: o caso da RNDS

De acordo com o *National Institute of Standards and Technology* (NIST), a computação em nuvem diz respeito a

> um modelo que permite acesso à rede de maneira conveniente e sob demanda a recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicativos e serviços) que podem ser rapidamente provisionados e liberados com o mínimo de esforço de gerenciamento ou interação com o provedor de serviços (NIST, 2011, p.6, tradução livre).

Esse recurso, comumente utilizado para facilitar a gestão de um quantitativo informacional elevado, vem sendo requisitado pelo governo brasileiro sob justificativa da necessidade de gerir, de maneira mais eficiente, os dados recolhidos de seus cidadãos, considerando-o, inclusive, como recurso estratégico (CETIC, 2021). O "Estudo Técnico Preliminar voltado à aquisição centralizada de serviços de computação em nuvem" publicado pelo Ministério da Economia em 2020 já menciona a intenção de investir grandes quantias na aquisição de Serviços em Nuvem - mais de duzentos e sessenta e três iniciativas de compras distintas, envolvendo novas contratações e renovações de contratos, cujo somatório aproxima-se de R$250 milhões (Ministério da Economia, 2020). Este mesmo Estudo nos mostra que o gasto previsto no planejamento de contratação desses serviços para o MS representava o valor mais elevado, cerca de R$ 14 milhões.

Movimento iniciado em 2018, a contratação de nuvens públicas deu-se a partir do Edital nº 29/2018 – serviços de computação em nuvem – vencido pela Empresa Brasileira de Telecomunicações (EMBRATEL), que ficou responsável pela intermediação e processo decisório envolvendo a contratação de serviços de computação em nuvem para diversos órgãos do Governo Federal, incluindo o Ministério da Saúde (ROSALES, 2020). Pouco depois, em 2019, foi firmada uma parceria junto ao MS para migrar os dados sensíveis da rede pública de saúde para a nuvem de armazenamento da *Big Tech* Amazon, para seu armazenamento e processamento (GROSSMAN, 2021).

Curiosamente, cerca de um ano depois desta operação, o então diretor do departamento de informática do Datasus, Jacson Barros, um dos responsáveis pelo processo de migração dos dados para a nuvem da empresa estrangeira, foi contratado pela própria Amazon para atuar como gerente de desenvolvimento de negócios estratégicos, conforme noticiado pelo portal Brasil de Fato (2022). Movimentação essa que, por sua vez, está registrada no próprio perfil do Linkedin – rede social voltada ao mercado de trabalho – de Jacson Barro**s,** conforme apresentado na figura abaixo:

Figura 02: Perfil do Linkedin de Jacson Barros.

Fonte: Linkedin, 2023.

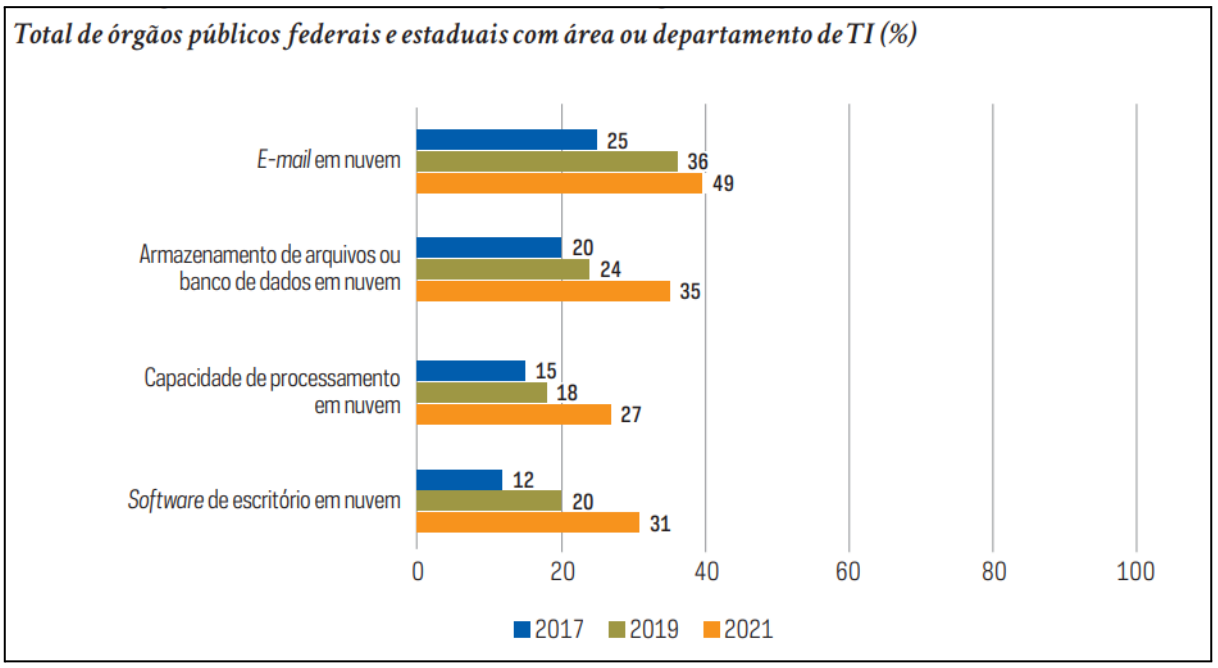
Além disso, na atual função de provedores de nuvem para a administração pública federal brasileira, encontram-se as empresas *Extreme Digital Solutions,* Huawei, Google e AWS – que, por sua vez, já abriga dados de cerca de 26 órgãos federais por conta do pregão

eletrônico nº 18/2020 (GROSSMAN, 2021), edital voltado a contratação de empresa especializada para prestação de serviços gerenciados de computação em nuvem. Companhias essas mencionadas que são, respectivamente, Brasileira, Chinesa e Norte-Americanas.

Conforme apontado pela Secretaria de Tecnologia da Informação e Comunicação (SETIC), é possível observar esforços para expandir a adoção de serviços baseados em infraestrutura de nuvem, como o acórdão TCU 1686/2019, o Decreto nº 10.332, de 28 de abril de 2020, e a Resolução nº 370 de 28/01/2021 (SETIC, 2022). Em resumo, estas resoluções buscam enfatizar, a sua maneira, que a contratação de serviços em nuvem trará benefícios para o setor público ao reduzir custos, simplificar a estrutura física, oferecer maior agilidade na entrega de serviços, dar suporte a iniciativas de *Big Data*, e melhorar a entrega de serviços para instituições públicas por meio da internet (SETIC, 2022). Portanto, como pode ser observado no texto do Decreto nº 10.332, que busca definir as estratégias voltadas para o desenvolvimento de um Governo Digital e sua consolidação, citado acima, recomenda-se que "órgãos e entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem" (BRASIL, 2020).

A vista disso, de acordo com o CETIC, tendo como base o ano de 2017, é possível observar um aumento na contratação de serviços de computação em nuvem em todos os níveis da administração pública (CETIC, 2021a). No que diz respeito aos serviços de armazenamento ou banco de dados em nuvem, o total de órgãos públicos federais e estaduais que contratam estes serviços aumentou de 20% para 35% no período de 2017 a 2021 e, de igual modo, a contratação de serviços de processamento em nuvem aumentou de 15% para 27% (CETIC, 2021a). É possível observar esses dados na figura abaixo.

Figura 03: Órgãos públicos federais e estaduais que contratam serviços de computação em nuvem, por tipo de serviço (2017, 2019 e 2021)



Fonte: CETIC, 2021a, p.84.

Não obstante, vale ressaltar que a contratação de serviços de armazenamento, em si, não se caracteriza como um problema. Porém, quando este serviço está destinado a um organismo federal e é terceirizado para empresas estrangeiras que possuem agendas e interesses próprios diferentes dos interesses e necessidades da população, faz-se necessário aplicar um olhar crítico. Essa discussão receberá maior atenção nas próximas seções do presente trabalho.

Dentre os fornecedores de serviços de armazenamento em nuvem para administração pública brasileira, destacam-se empresas internacionais como Amazon, Google e Microsoft, concentrando 24% dos fornecedores, sendo a Amazon a maior destas (JUNIOR, 2020). Vale ressaltar que estas empresas internacionais, gigantes no campo da tecnologia, também detêm grande parte deste mercado em outros países, o que demonstra sua predominância neste mercado (Paquette et al., 2010; El-Gazzar & Wahid, 2015; Yang & Tate, 2012; apud JUNIOR, 2020).

Portanto, observa-se que o mercado de armazenamento já vem sendo dominado por este grupo seleto de empresas, que utiliza de seu capital, complexidade técnica e domínio das infraestruturas físicas e digitais para expandir suas operações e prevalecer sobre concorrentes.

Dados da Statista (2023) nos mostram que 65% destes serviços em escala global partem das mesmas empresas mencionadas acima, contratadas por governos, outras empresas e pessoas físicas.

Por meio desse domínio, tornam-se capazes de prejudicar o desenvolvimento local, comandar o mercado e extrair receitas dos países em desenvolvimento. Isto pois, como possuem maiores recursos financeiros, somado ao fato de já estarem consolidadas no mercado, conseguem adotar práticas para eliminar ou enfraquecer a concorrência, como preços extremamente competitivos, assim como promover a criação de barreiras à entrada de novos concorrentes; ao mesmo tempo, são capazes de fortalecer sua posição no mercado por meio da aquisição dessas empresas menores, criando verdadeiros monopólios. Portanto, é necessário estar atento às consequências de optar por seus serviços, conforme será melhor discutido ao nos debruçarmos sobre o conceito de 'colonialismo digital' no próximo capítulo.

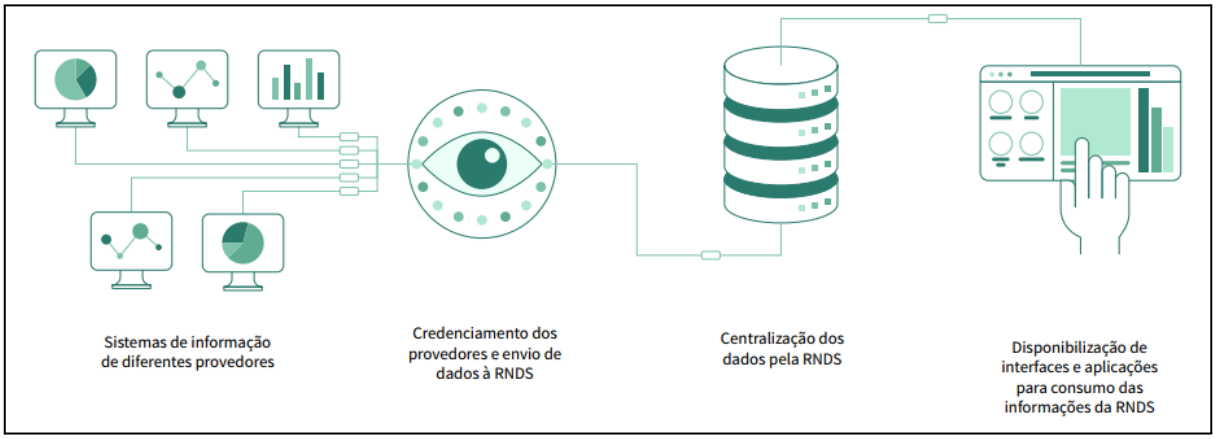
De acordo com Avelino (2021), o principal objetivo das empresas que fornecem serviços em nuvem é incentivar quem as contrata a externalizar todo seu negócio para seus servidores e, com isso, seus monopólios criam dependência de seus serviços. Deste modo, embora a adoção destes serviços por parte do Governo Federal justifique-se na busca pelo aumento de eficiência dos serviços prestados, de maneira a simplificar a estrutura física e reduzir custos, ainda é necessário ter atenção e preocupação com a segurança destes dados que estão sendo processados, "como riscos tangíveis que conseguem ser controlados e riscos intangíveis, que fogem do controle dos gestores da aplicação" (JUNIOR, 2020, p.33), haja vista a complexidade do compartilhamento das informações de saúde.

Esse compartilhamento inseguro e até mesmo o vazamento de informações sensíveis podem ser extremamente prejudiciais aos usuários, posto que, além da exposição de dados como CPF, endereço, telefone e histórico de doenças, que podem ser facilmente aproveitados por empresas e pessoas com intenções maliciosas para golpes e fraudes, pode resultar até mesmo em enfermidades. De acordo com o *Ponemon Institute* (2022), companhia voltada a pesquisa independente na área de cibersegurança, quando este vazamento de informações e ataques cibernéticos impactam os tratamento saúde nos hospitais e centros de atendimento, observa-se um aumento de até 24% nas taxas de mortalidade dos pacientes (Ponemon Institute, 2022, p. 34).

À vista disso, armazenada em servidor de uma destas *Big Techs*, encontra-se a Rede Nacional de Dados em Saúde (RNDS), plataforma que visa tornar mais claro e eficiente o fluxo de informações coletadas pelos diversos centros de saúde espalhados pelo Brasil,

facilitando sua interpretação e padronização por meio de um novo sistema de gestão, como pode ser observado:

Figura 04: Rede Nacional de Dados em Saúde



Fonte: Instituto de Estudos para Políticas de Saúde (IEPS), 2023, p.11.

Como ilustrado acima, os provedores, ou seja, os diversos estabelecimentos de saúde e laboratórios, integram-se a RNDS a partir dos diferentes Sistemas de Informação em Saúde que utilizam. Essa integração, por sua vez, ocorre por meio de *software* denominado FHIR (*Fast Healthcare Interoperability Resources*), que apresenta um padrão para troca de informação em saúde e permite interoperabilidade com a RNDS (BRASIL, 2023)[2]. A partir daí, informações como registros de atendimentos, medicamentos em uso ou utilizados pelos pacientes, exames, histórico de internações etc, cadastradas por esses provedores, acabam centralizadas e armazenadas na RNDS e, por fim, podem ser consultadas com mais facilidade, por exemplo, por meio do 'Portal de Serviços do DataSUS'[3].

De acordo com pesquisa realizada por Coelho-Neto e Chioro (2021), "no Brasil existem mais de 50 sistemas de base nacional, e a fragmentação resulta em um olhar voltado especificamente para as doenças ao invés de um olhar que observe a saúde de forma integrada" (COELHO-NETO e CHIORO, 2021, apud Rachid et al, 2022). Portanto, por meio da RNDS, o MS busca superar a existência de uma quantidade elevada de sistemas de informação em saúde (SIS) – como por exemplo Cartão Nacional de Saúde (CNS), o Sistema de Informação em Saúde para a Atenção Básica (SISAB), a Base Nacional de Notificações (BNN) etc (CUNHA e VARGENS, 2017) – e a forma como estas informações são coletadas, de maneira a centralizá-las em uma única base de dados, buscando proporcionar o acesso mais

[2] Para mais informações sobre o funcionamento da RNDS acesse: Ministério da Saúde - Guia RNDS.
[3] Portal de Serviços do DataSUS. Disponível em: https://servicos-datasus.saude.gov.br.

rápido a essas informações e, consequentemente, promover o desenvolvimento de políticas públicas de saúde mais abrangentes.

2.6 – Críticas a alocação da RNDS na nuvem de armazenamento da Amazon

Conforme apresentado, a RNDS visa materializar as metas desenvolvidas pelas estratégias de SD que a conceberam, aplicando um discurso de desenvolvimento e utilização de tecnologias inovadoras, gestão de dados, inteligência artificial e armazenamento em nuvem para melhorar os atendimentos médicos no Brasil. Assim, antes de discutirmos as vulnerabilidades presentes na alocação da RNDS na nuvem de armazenamento da Amazon, à luz do do colonialismo digital, cabe primeiramente apresentar as críticas que vêm cercando o desenvolvimento do projeto.

Primeiramente, argumenta-se que o desenvolvimento da RNDS foi pouco discutido, posto que o processo de consulta pública e contribuições para o projeto foram insuficientes, somente quinze dias, de maneira a limitar a participação democrática (FORNAZIN, 2022, apud PASSOS, 2022). Também se observa que ela não se propõe a registrar algumas informações essenciais para o desenvolvimento de políticas públicas de saúde, como dados sociais e ambientais, o que acaba por reduzir a efetividade das políticas públicas que se baseiam em seus diagnósticos (DIÓGENES e RIBEIRO, 2023).

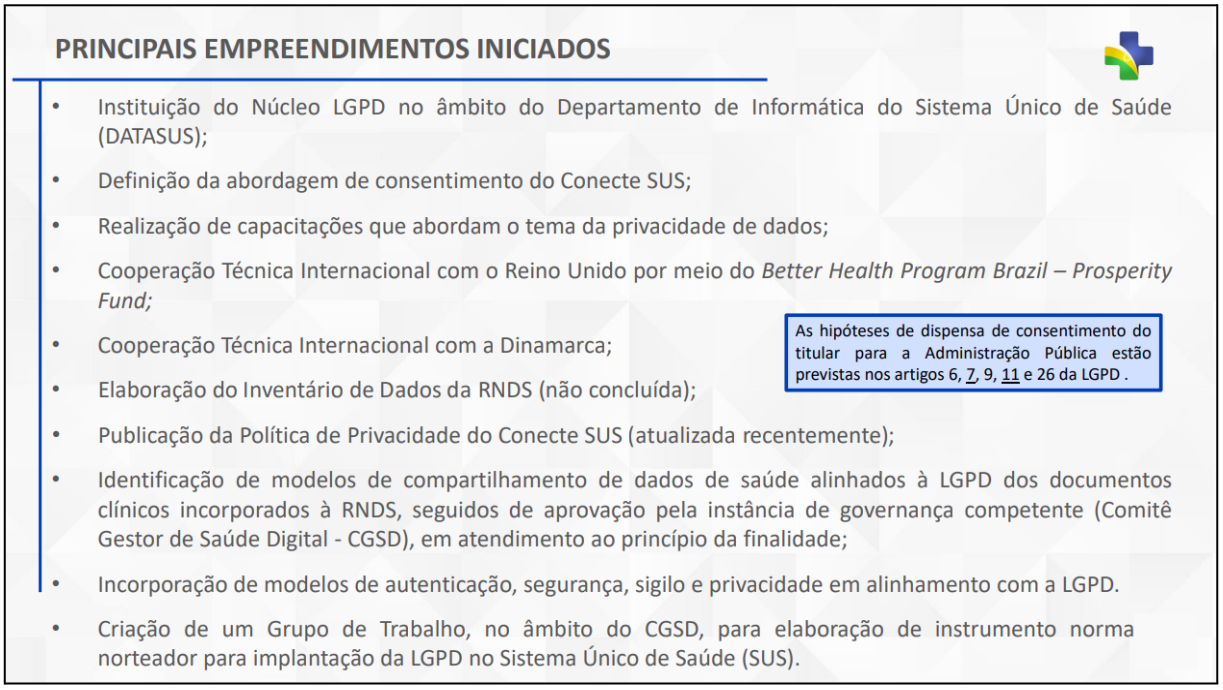
Além disso, destaca-se que RNDS atravessa princípios constitucionais e do SUS ao centralizar todas as informações em seu banco de dados único, limitando os Estados da Federação ao acesso direto a suas próprias informações e levando-os a recorrer a contratação de suporte ou autorização do MS para obtê-los (FORNAZIN, 2022, apud PASSOS, 2022). Logo, haja vista essa concentração de dados, intensificam-se as consequências caso ocorra uma falha de segurança, pois uma enorme quantidade de informações pode ser acessada de uma só vez e, de igual modo, um ‘apagamento’ dessa base levará consigo uma quantidade elevada de informações (FORNAZIN, 2022, apud PASSOS, 2022).

Ademais, há também preocupações sobre a forma como os dados do SUS são protegidos em relação ao setor privado pela RNDS, visto que não há clareza sobre o trâmite de troca de informações entre pacientes, hospitais e empresas, somente há informação de que elas são compartilhadas; preocupações essas que, inclusive, se intensificam ao compreendermos que a RNDS segue caminhando para alcançar conformidade às exigências da LGPD, visto que ainda possui falhas no que concerne a interoperabilidade dos dados por ela armazenados (PINTO, 2022, apud PASSOS, 2022; RACHID et al, 2022). Isto pois, a

RNDS, por ser um centralizador que pretende a integração de dados em saúde, não foi projetada com o intuito específico de interoperabilidade dos dados, conforme prescreve a LGPD atual (Fantonelli et al, 2020).

Não obstante, em 2022, três anos após o início da implementação da RNDS em escala nacional, ainda discutia-se no MS os aspectos gerais para adequação da RNDS à LGPD, conforme pôde ser presenciado na "Oficina de Expansão do Programa Conecte SUS – Goiás/GO"[4], evento que ocorreu em novembro do mesmo ano, buscando discutir temas relacionados a 'ESD 28' e a implementação do Conecte SUS. Ao analisarmos às apresentações que ocorreram nessa ocasião, do qual a figura 05, abaixo, foi retirada, observa-se que os seguintes pontos ainda estão em fase de desenvolvimento na consolidação do projeto:

Figura 05: Slide da Oficina de Expansão do Conecte SUS de 2022.



Fonte: Ministério da Saúde, 2022.

Portanto, compreendemos que desde sua implementação a RNDS vêm operando sem estar 100% em conformidade com as exigências estabelecidas pela LGPD, ainda que esteja caminhando para tal. Somado a isso, temos que os dados que nela são registrados vêm, desde 2019, sendo armazenados e processados nos servidores de uma multinacional estrangeira, que

[4] Para verificar a apresentação de slides por completo, acesse: https://cosemsgo.org.br/wp-content/uploads/2022/11/Aspectos-Gerais-para-adequacao-da-RNDS-a-LGPD.pdf

possui interesses e agenda própria, portanto, informações sensíveis da população brasileira, essenciais para o desenvolvimento de políticas públicas pelo governo federal, estão nas mãos de uma empresa multinacional norte-americana. Como é destacado no próximo capítulo, temos escancarado e intensificado o ‘colonialismo digital’.

3 - Colonialismo Digital *vs.* Soberania Digital

3.1 - O que é o colonialismo digital e como podemos observá-lo na prática

Embora o desenvolvimento tecnológico traga inúmeros benefícios, como a ampla conectividade, facilidade de acessar informações, aumento da eficiência, redução dos custos de diversos serviços e, especificamente no campo da saúde, técnicas que visam aprimorar atendimentos, diagnósticos e pesquisas, também é preciso aplicar um olhar crítico sobre a maneira pela qual estas tecnologias são utilizadas e suas consequências. Isto pois, este mesmo desenvolvimento, que vem sendo construído e atrelado a um modelo de pensamento neoliberal – visto o avanço do setor privado na esfera pública – tem ampliado e aprofundado novas formas de colonialidade, como o 'colonialismo digital' (AMADEU, 2022).

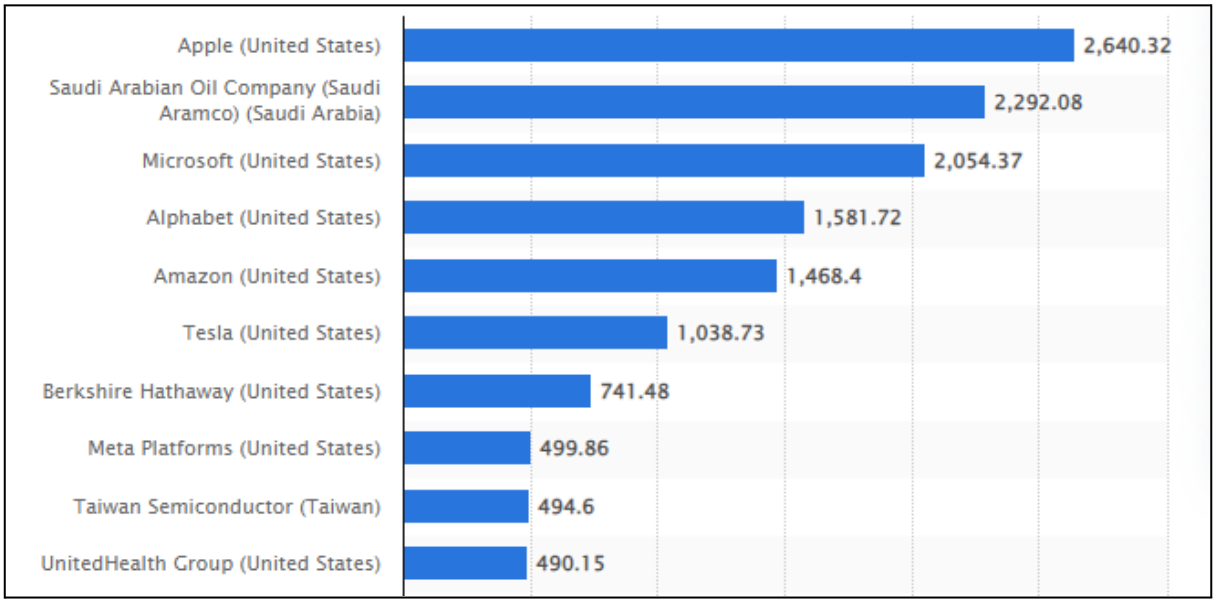
Este avanço, por sua vez, representa uma face recente do neoliberalismo, denominada "fornecimento privado de bens públicos ou a redistribuição privada de lucros para causas sociais" (BARON, 2009, p.1, tradução livre), onde as empresas, por interesse próprio, de maneira voluntária ou em resposta a pressões sociais, buscam se beneficiar de um 'desempenho social positivo'. Ao se posicionarem no mercado como empresas de boa reputação, tornam-se capazes de cobrar preços mais altos por seus produtos, possuem maior poder de barganha, recebem menos pressão de ativistas sociais e da opinião pública, são mais valorizadas no mercado de ações e atraem uma maior quantidade de investimentos de acionistas (BARON, 2009). Portanto, procuram assumir uma responsabilidade que normalmente é atribuída ao Estado, como a oferta de bens públicos, com baixos riscos e oportunidades de retorno positivo; além disso, quanto maior a empresa, maior a probabilidade de se envolver nesse fornecimento (BERNHAGEN e MITCHELL, 2010).

Pois bem, primeiramente, o colonialismo pode ser compreendido como uma relação específica de poder, onde, por meio da expropriação econômica, cultural, territorial, dos recursos naturais e corpos dos cidadãos de determinada localidade, ocorre a dominação de uma nação sobre a outra (MARRANO, 2021). Nesta dominação, perpetrada e legitimada por uma relação assimétrica de forças entre o Estado colonizado e o colonizador, busca-se, por meio da retirada de riquezas, explorar o mais fraco para obter vantagens no mercado internacional. Além disso, utiliza de um falso discurso civilizatório para invadir terras 'inexploradas' e torná-las economicamente ativas, de maneira a justificar sua exploração e imposição de uma lógica capitalista (ASSIS, 2014). Infelizmente, as sequelas deste sistema de dominação ainda se fazem presentes, e apresentam-se por meio da colonialidade.

Conforme elaborado por Assis (2014), a colonialidade diz respeito a novas formas de dominação, que extrapolam as particularidades do colonialismo e se mantêm presentes mesmo após a descolonização. Portanto, "é a continuidade da propagação do pensamento colonial, sendo uma matriz que se expressa essencialmente em relações dominantes de poder, saber e ser, reproduzidos cotidianamente" (BALLESTRIN, 2013, p.1 apud AVILA, 2021). A colonialidade se faz presente na dimensão simbólica, e naturaliza uma estrutura hierárquica, de conhecimento e relações de poder. Sem ela não há a modernidade, não há a lógica capitalista (TONIAL et al, 2017). Em síntese, a colonialidade é o elemento que se mantém presente mesmo após a retirada do colonizador, posto que o processo de dominação exercido por ele extrapola as barreiras físicas, culminando na reprodução cotidiana de comportamentos e pensamentos impostos nessas relações coloniais, resultando na manutenção da lógica neoliberal.

Não obstante, no que diz respeito aos recursos buscados pelos colonizadores, temos que estes sofreram alterações ao longo dos anos, observadas as mudanças trazidas pelas tecnologias e as necessidades de cada período. Ao recorrermos ao colonialismo histórico, com o desenvolvimento da lógica mercantilista impulsionada pela expansão marítima europeia, observamos o forte interesse em usurpar as especiarias e metais preciosos do Oriente e das Américas, como por exemplo pau-brasil, café, açúcar, prata, ouro etc (DUARTE e GRACIOLLI, 2017). Posteriormente, frente a expansão industrial capitalista, o foco alterou-se para recursos como cobre, carvão e, mais tarde, o "ouro negro" – também conhecido como petróleo – para alimentar as fábricas (LAINE, 2009). Porém, devido a constante evolução das tecnologias e suas aplicações, conforme apresentado pelo jornal *The Economist* em matéria publicada em maio de 2017, o recurso mais valioso do mundo não é mais o petróleo, mas sim os dados, que agora se tornaram matéria-prima para as tecnologias digitais, produtoras de valor (THE ECONOMIST, 2017). Esta relação é bem representada na figura abaixo:

Figura 06: Maiores empresas por capitalização de mercado em 2022



Fonte: STATISTA, 2022.

Na figura, é possível observar que, dentre as dez empresas que apresentaram maior valor de mercado em escala global no ano de 2022, seis delas são as chamadas *Big Techs* do Vale do Silício, demonstrando a dimensão e influência que as companhias de tecnologia exercem atualmente, similar a predominância das gigantes do ramo petrolífero e energia, como a Exxon, Total, e Shell, que dominavam em valor de mercado no início do século XX (THE ECONOMIST, 2017). As principais empresas de tecnologia, também conhecidas como *Big Five* – Microsoft, Apple, Amazon, Alphabet, e Meta – somaram juntas em receita, no ano de 2019, um valor maior que o PIB de quatro nações do G20 e, caso fossem analisadas como um único país, ocupariam a décima oitava posição no ranking das maiores economias do mundo no mesmo ano (PICKERT, 2022). Consequentemente, o avanço tecnológico no campo da comunicação e a crescente utilização de tecnologias digitais deu origem a novas formas de controle e dominação por estas grandes empresas, criando dependência de suas plataformas e dos dados que elas conseguem recolher, resultando numa dinâmica denominada 'colonialismo digital'.

3.2 - Colonialismo digital, a nova face do capitalismo neoliberal?

O colonialismo digital é reflexo do atual modelo de produção capitalista (FAUSTINO e LIPPOLD, 2022). De acordo com Kwet (2019), ele pode ser compreendido como uma

forma estrutural de dominação, por meio da propriedade e domínio centralizado das estruturas físicas, da própria conectividade de rede e suas informações pelas gigantes de tecnologia, que detém seu monopólio. Por meio dele,

> corporações estrangeiras prejudicam o desenvolvimento local, dominam o mercado e extraem receita do Sul Global, com poder obtido principalmente por meio da dominação estrutural da arquitetura digital, o que leva a formas mais gerais de controle imperial (KWET, 2019, p.5, tradução livre).

Portanto, por meio da sua própria arquitetura digital, desenvolvida para suprir suas próprias necessidades, as *Big Techs* impõem mecanismos privados de governança que culminam numa dominação econômica e cultural dos países em desenvolvimento, exercendo influência direta sobre as relações políticas, econômicas e sociais, assim como sobre o fluxo de informações que ocorre por meio de suas plataformas (KWET, 2019). Ao mesmo tempo, essas grandes corporações articulam-se para dificultar que novos participantes consigam adentrar seu mercado, controlando as estruturas físicas (cabos, servidores, transmissores, fontes de matéria prima) e o recurso intelectual – ao realizarem parcerias com universidades – contratando as melhores mentes para continuar desenvolvendo seu domínio (SIQUEIRA, 2019). Logo,

> na economia de dados, isso se manifesta na impossibilidade de até mesmo tratar os dados das empresas e da sociedade nos próprios territórios e em instituições e empresas locais. A fusão do ordenamento neoliberal com as teias de colonialidade sustentam a posição de eterno dependente das tecnologias criadas na matriz (AMADEU, Sergio, 2022, p.49).

Deste modo, o tipo de dominação que ocorre agora é por meio do controle da tecnologia, dos dados e das ferramentas que os coletam, criando uma situação de dependência por meio de práticas computacionais extrativistas que, com esses dados, multiplicam o lucro privado (SIQUEIRA, 2019). Estas últimas, por exemplo, podem ser identificadas nas interações entre seres humanos e tecnologias digitais, que acabam por produzir registros, rastros e dados que serão recolhidos, armazenados, analisados e utilizados por essas mesmas empresas para conversão em lucro por meio de produtos e serviços personalizados, com ou sem a consciência dos usuários.

Concomitantemente, também é possível observar uma forte presença do ‘Dataísmo’ – ou filosofia dos dados – que diz respeito à cega confiança nos algoritmos e mecanismos de inteligência artificial, causando uma falsa percepção da realidade, onde desenvolve-se uma visão de que tudo pode e deve ser quantificado (KAUFMAN e SANTAELLA, 2021).

Não obstante, conforme apresentado por Amadeu (2022), os resquícios de colonialidade na era de acumulação informacional acabam por gerar “polos de ofuscamento” (AMADEU, Sergio, 2022 p.45) – ou seja, a crença de que essas empresas de tecnologia

existem somente para nos servir, somada à impossibilidade de compreender os efeitos negativos das tecnologias –, e podem ser observados na ausência e impossibilidade de reflexão sobre a forma como estas gigantes de tecnologia incidem sobre a vida cotidiana, apresentadas, segundo o autor, em crenças como: (i) empresas e plataformas digitais são neutras e não interferem no dia a dia das populações; (ii) inexistência de consequências negativas locais e nacionais na utilização da arquitetura digital das *Big Techs*; (iii) os dados coletados dos cidadãos de países em desenvolvimento possuem os mesmos efeitos econômicos, políticos e sociais dos cidadãos dos países detentores e produtores das tecnologias informacionais (AMADEU, 2022). Com isso, esses 'polos de ofuscamento' se apresentam como consequências da colonialidade, produzindo alienação e distanciando a população das reflexões sobre os resultados desta coleta massiva de dados (AMADEU, 2022).

Outro ponto fundamental do colonialismo de dados se apresenta nos novos processos de acumulação e apropriação de valor, atualizados com o surgimento das *Big Techs* e suas práticas computacionais extrativistas (FAUSTINO e LIPPOLD, 2022). Isto pois, ao monopolizar os meios de produção, como estruturas físicas, digitais, cabos, servidores, programas e diversos outros produtos, as *Big Techs* intensificam e atualizam métodos de apropriação e acumulação de capital ao tornarem diversos setores da economia, pertencentes ou não a administração pública, dependentes de seus produtos e serviços (FAUSTINO e LIPPOLD, 2022). Além disso, observa-se que a arquitetura jurídica, nacional e internacional, apresenta barreiras aos países em desenvolvimento que procuram estimular políticas que visam a produção e compra de bens e serviços produzidos domesticamente (PINTO, 2018).

Portanto, percebe-se que esse processo envolve uma disputa assimétrica de forças, onde o progresso das tecnologias digitais verdadeiramente nacionais dos países em desenvolvimento, oriundas de uma arquitetura digital criada e impulsionada por seus próprios algoritmos e dados, é limitado é aprisionado pelas regras estabelecidas pelos países desenvolvidos do 'Norte-Global', sendo essa mais uma barreira de entrada, que aprofunda as desigualdades e escancara os diferentes níveis de avanço tecnológico.

Conforme exposto anteriormente, esse processo de intensificação da extração de dados ocorre principalmente nos países em desenvolvimento que são caracterizados pelo estigma do 'Sul Global', reduzindo-os a territórios de extração dessas informações e consumidores de tecnologia externa, além de empobrecê-los (FAUSTINO e LIPPOLD, 2022). Assim, por meio deste processo de acumulação,

> dados sigilosos dos sistemas de saúde, educacional e de justiça, redes públicas de educação, entre outros, têm sido sistematicamente sugados pelo

> pelos grandes monopólios informacionais (SILVEIRA, 2020, apud FAUSTINO E LIPPOLD, 2022),

e posteriormente convertidos em lucro para as gigantes da tecnologia. Neste processo, os dados absorvidos pelas *Big Techs* são utilizados para criar perfis, com o maior detalhamento possível, para que elas tenham uma melhor compreensão de quem é o consumidor e no que ele está interessado (GOSWAMI, 2022; SOLVER, 2021). Paulatinamente, por meio de algoritmos, tornam as interações com o consumidor tão relevantes e personalizadas quanto possível, oferecendo produtos, serviços e anúncios que possam gerar interesse, baseado em suas últimas atividades; além disso, essas empresas são as próprias geradoras de interesse, induzindo os usuários a certos comportamentos por meio dessas abordagens personalizadas, se beneficiando da manipulação (GOSWAMI, 2022; SOLVER, 2021).

Por exemplo, o colonialismo digital pode ser observado, conforme alertado por Kwet (2019), na predominância que os serviços oferecidos pelas gigantes de tecnologia estadunidenses possuem no contexto global: a ferramenta de pesquisa do Google, da empresa Alphabet, recebe cerca de 89,3 bilhões de visitas mensais, e representou mais de 80% da participação de mercado em abril de 2023. O navegador Google Chrome correspondeu a 63% da participação no mercado global de navegadores, seguido pelo Safari, da Apple, com 21% de participação em maio de 2023. No que diz respeito a sistemas operacionais para computadores, o Microsoft Windows representou mais de 70% de participação de mercado em janeiro de 2023 (todos esses dados estão em STATISTA, 2023). Os serviços de computação em nuvem também foram dominados pelas *Big Techs* Amazon, Microsoft e Google, que até maio de 2023 representaram 66% do mercado global (GRIFFITHS, 2023). Além destes destacados, é possível observar a predominância estadunidense nos sistemas operacionais de celulares, ferramentas computacionais para empresas, serviços de marketing, redes sociais etc (KWET, 2019).

Outro exemplo do poder que reside nas mãos dessas grandes empresas foi apontado por Epstein (2016), que observou que a gigante Google - por meio de sua ferramenta de pesquisa, ao induzir seus usuários a determinadas publicações e artigos com informações favoráveis ou desfavoráveis a um candidato, ou até mesmo pelo bombardeio de publicidades pagas, supridas de viés político - é capaz de influenciar os votos nas eleições em qualquer país que as utilize, podendo manipular as preferências de voto de 80% dos eleitores em certos grupos demográficos (EPSTEIN, 2016).

Na área da Saúde, conforme apresentado por Souza (2022), também é possível enxergar as facetas dessas práticas extrativistas, que se aproveitam do desenvolvimento

tecnológico para conversão de dados em lucro. De acordo com a autora, embora neste campo a utilização de sistemas de categorização, como estatísticas da população relacionadas a idade, sexo, condições físicas, histórico de doenças e saúde etc, de maneira geral já sejam utilizadas para o desenvolvimento de políticas públicas, o avanço das tecnologias digitais na área intensifica as formas de controle e poder que esses sistemas de coleta de informações podem desempenhar (SOUZA, 2022).

Frente à crescente participação do setor privado, por meio de serviços oferecidos por *Big Techs* e *health techs*, inova-se na maneira como os dados são recolhidos, haja vista a crescente tendência de utilização de aplicativos móveis e dispositivos eletrônicos para auxiliar no monitoramento das taxas de saúde, como frequência de atividades físicas, padrões de sono, batimentos cardíacos etc. Assim, observa-se uma estratégia lucrativa para empresas que, por meio deste monitoramento, criam perfis detalhados dos usuários, possibilitando direcionar anúncios personalizados, oferecer serviços e produtos relacionados à saúde, e até mesmo vender ou compartilhar os dados com terceiros. Com isso, "a vida humana não está apenas anexada ao capitalismo, mas também fica sujeita ao monitoramento e a vigilância contínuos" (SOUZA, Joyce, 2022, p.119).

Observamos que esse processo é, portanto, bastante preocupante, pois também aprofunda o sentimento de que não há escapatória dessas grandes empresas, posto que a própria vida se torna uma *commodity*. Conforme discutido, estamos aprisionados em relações, intencionais ou não, com máquinas e ferramentas digitais programadas para a todo momento aprender mais sobre como nos comportamos.

Isto é justamente o que a autora Shoshana Zuboff (2019) define como 'capitalismo de vigilância', um novo modelo de capitalismo baseado na extração de dados pessoais e sua utilização para fins comerciais. Sob justificativa de que a coletada de dados possui como principal objetivo a melhora da oferta e qualidade dos serviços, as *Big Techs* utilizam os 'rastros' deixados pelos usuários nas mais diferentes interações com as tecnologias para alimentar inteligências artificiais (IA) e construir perfis assertivos do comportamento humano. Nesta dinâmica, segundo a autora, todos somos constantemente monitorados, e os dados presentes nesses 'rastros' são utilizados para manutenção da lógica capitalista ao serem transformados em capital e poder econômico. Ao mesmo tempo, os dados extraídos nessas interações são vendidos por terceiros, que por sua vez vendem a terceiros, e assim sucessivamente, tornando praticamente impossível a responsabilização e localização de todos os envolvidos no processo. Como diz a autora, "com essa lógica, a experiência humana é

mercantilizada pelo capitalismo de vigilância, para renascer como 'comportamento'" (ZUBOFF, Shoshana, 2019, p.1).

3.3 – É possível reagir ao colonialismo digital?

Exemplos de soberania digital: o Plano CEIBAL no Uruguai e o Programa de Emergência para a Soberania Digital no Brasil

A coleta massiva de dados realizada pelas empresas de tecnologia é cada vez mais agressiva, capaz de tornar os mais diversos aspectos da vida humana em informações para serem convertidas em lucro. Isso tem gerado preocupações em diferentes Estados, motivando discussões acerca de como garantir sua autonomia tecnológica e 'soberania digital' (BARRIOS, 2023). Soberania digital pode ser compreendida como a capacidade do Estado de exercer sua soberania no espaço virtual, de maneira a garantir que sua autoridade – seu poder administrativo e jurisdições – seja respeitada, além de outros elementos como a proteção de dados sensíveis dos usuários e a não subordinação às empresas de tecnologia (AMIOT et al, 2020; DERIVRY, 2023). Assim, buscar essa soberania apresenta-se como fundamental, visto que "países inteiros e suas indústrias são totalmente dependentes de infraestrutura, softwares e hardwares essenciais fornecidos por poucas empresas sediadas em um pequeno grupo de países" (PINTO, Renata, 2018, p.20).

Para Pinto (2018), ciente dessa dependência, é urgente a conscientização dos Estados para o fomento e financiamento de iniciativas locais que desenvolvam habilidades, técnicas e ferramentas alternativas, assim como o investimento em tecnologias comunitárias e o intercâmbio de conhecimento entre os países em desenvolvimento do Sul Global (PINTO, 2018). Como exemplo dessas iniciativas, há o Plano CEIBAL (*Plan de Conectividad Educativa de Informática Básica para el Aprendizaje en Línea*), do Uruguai, política pública de inclusão social e digital que, por meio de iniciativas comunitárias, buscou ampliar o acesso da população a tecnologias e o próprio acesso à internet em locais públicos, como as praças, de maneira a repensar relações de consumo (NAVARRETE, 2014).

Através dessa política, o governo uruguaio permitiu aos alunos em idade escolar um laptop próprio, incentivando-os a participar de projetos que os estimulam física e psicologicamente a interagir com as tecnologias em conjunto com as cidades onde vivem, fomentando um sentimento coletivo e autônomo. Além disso, outra iniciativa deste plano foi migrar todo sistema educacional uruguaio para um software de código aberto, ou seja, disponível para todos, incentivando a colaboração entre desenvolvedores e estimulando a

produção de tecnologias locais (PINTO, 2018). A partir dessa política, que apresenta uma forma diferente de interação numa sociedade digital via incentivo do senso comunitário, podemos questionar as manifestações da lógica neoliberal (NAVARRETE, 2014). Portanto, questiona o individualismo, o materialismo e a redução de investimentos sociais perpetrados pelo modelo econômico capitalista.

Também vale ressaltar um exemplo brasileiro onde, em agosto de 2022, cientes desta problemática entre *Big Techs* e Estado, acadêmicos e ativistas brasileiros elaboraram o "Programa de emergência para a Soberania Digital", carta aberta destinada a Lula, então candidato à presidência, apresentando iniciativas para tornar mais robusto o ecossistema tecnológico nacional, com objetivo de "tirar o Brasil do atual papel subalterno, restabelecendo seu papel de líder regional na adoção de políticas de tecnologia da informação que busquem pela justiça social" (EVANGELISTA, Rafael, 2022, p.1).

Assim, de maneira a proteger o país das ameaças apresentadas pelas grandes empresas de tecnologia, reconhecendo que dados sensíveis da população vêm sendo extraídos do país para alimentar algoritmos, a carta propõe medidas para potencializar uma transformação digital no país. Dentre elas, destacam-se: desenvolvimento de tecnologia e infraestrutura nacional para hospedagem de dados, seguindo os termos da LGPD; fomento a formação interdisciplinar, ética e de permanência de cientistas e técnicos, para desenvolvimento de tecnologias de IA; e incentivo e financiamento para tecnologias locais que visem superar as desigualdades e dependências perpetuadas pelas *Big Techs* (EVANGELISTA, 2022). Estas medidas visam fortalecer a posição do Brasil no cenário digital, promovendo sua independência tecnológica e garantindo a proteção dos dados e informações da população.

Portanto, iniciativas como o Plano CEIBAL e o Programa de Emergência para a Soberania Digital surgem para oferecer alternativas que fujam da atual lógica neoliberal e suas ameaças - onde as empresas se apresentam na posição de desenvolver, produzir e comercializar as tecnologias digitais, enquanto os Estados (que possuem a capacidade de regulamentar, tributar e incentivar ou não o consumo público do que é oferecido por tais empresas) têm reconhecidas as suas limitações e dependência dessas ferramentas, se vendo cada vez mais reféns de suas infraestruturas (FLORIDI, 2020, p.371).

Exemplo claro destas ameaças pôde ser presenciado nas últimas eleições presidenciais brasileiras, tanto em 2018 quanto 2022, momento em que notícias falsas, apelidadas de *fake news*, circularam sem controle pelas redes sociais, impulsionadas pelos algoritmos das *Big Techs*. Elas entregaram aos seus usuários conteúdos personalizados, carentes de conexão com a realidade dos fatos, fomentando a desinformação e a 'ruptura institucional', conforme

elencado pelo Tribunal Superior Eleitoral (TSE). O ápice desse movimento materializou-se no dia 08 de janeiro de 2023, quando grupos da extrema direita, revoltosos com os resultados do processo democrático e munidos de desinformação, marcharam em direção a prédios do governo federal em Brasília, como o Palácio do Planalto, o Palácio do Congresso Nacional e o Palácio do Supremo Tribunal Federal, vandalizando e depredando patrimônio público, visando a derrocada do Estado Democrático de Direito (CARDOSO et al, 2023).

3.4 – A trajetória normativa brasileira na busca pela Soberania Digital

Com isso, é possível observar uma mobilização da administração pública federal brasileira para incidir sobre este processo de transformação digital, de maneira a conduzi-lo, posto que o 'dataísmo' e a falta de controle na circulação desses dados constituem ameaças ao funcionamento do regime democrático, haja vista os exemplos apresentados acima, além de prejudicarem o desenvolvimento da autonomia e do mercado interno (BARRIOS, 2023). Assim, conforme apresentado por Barrios (2023), os esforços para guiar a transformação digital brasileira podem ser observados principalmente nas seguintes políticas do governo: (i) o Marco Civil da Internet – MCI (Lei nº 12.965/2014); (ii) Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018); e (iii) Estratégia Brasileira para a Transformação Digital, políticas essas complementares entre si.

Primeiramente, o Marco Civil da Internet (MCI**)**, sancionado em 2014, representa o início do movimento de proteção aos dados pessoais dos brasileiros. Buscou definir os direitos e deveres dos usuários, de maneira a apresentar princípios para o uso da internet (SANTOS, 2019). Nele, destacam-se iniciativas voltadas a (i) neutralidade de rede, procurando garantir que os dados em tráfego recebam tratamento igual pelos provedores; (ii) obrigações para esses provedores, definindo sua responsabilidade de armazenar determinadas informações para auxiliar em investigações policiais, reforçando a autoridade do Estado nesse espaço; e (iii) a privacidade dos usuários e sua liberdade de expressão (BRASIL, Congresso, 2014).

Porém, o MCI pouco discutiu acerca da responsabilidade das plataformas sobre o que nelas trafega, o que permitiu a proliferação e disseminação de desinformação pelas mesmas (SANTOS, 2021) - fato observado com o avanço das *fake news*. Além disso, na construção do MCI havia um projeto que visava, por meio de decreto, uma exigência aos provedores estrangeiros de instalar ou utilizar *data centers* em território nacional para tratar e armazenar

os dados dos cidadãos brasileiros no Brasil, no objetivo de dificultar / evitar a espionagem eletrônica (BLUM e VAINZOF, 2014).

Infelizmente, essas medidas não avançaram, visto que o então líder do PMDB na Câmara – partido de oposição ao governo que na época possuía a segunda maior bancada do Congresso –, Eduardo Cunha, argumentava que as empresas de tecnologia teriam seus custos aumentados, o que se tornaria um possível entrave a sua entrada no país (CALGARO, 2014). Nesse momento foi colocado, portanto, o bem-estar das companhias acima da proteção de dados dos cidadãos brasileiros e o incentivo à soberania nacional sobre esses dados.

Por sua vez, a Lei Geral de Proteção de Dados Pessoais (LGPD) buscou complementar e reforçar os parâmetros estabelecidos em princípio pelo MCI, representando um importante marco para a garantia da proteção dos dados. Principalmente, a LGPD visa equilibrar o poder econômico e político resultante do uso abusivo das informações pessoais coletadas, protegendo os direitos dos usuários, dando destaque, em especial, a regulação da transferência internacional de dados (BARRIOS, 2023). Além disso, delega a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), "entidade da administração pública federal indireta, submetida a regime autárquico" (BRASIL, 2023, p.1), a responsabilidade de reforçar e fiscalizar estes princípios.

Todavia, conforme elaborado por Bastos et al (2021), embora a LGPD desempenhe um papel fundamental, apresentando um arcabouço jurídico robusto para proteção dos dados pessoais, seus críticos argumentam que seu atual modelo é ineficiente para lidar com as mudanças impostas pelas novas tecnologias, visto que a LGPD reduziu a

> importância ao consentimento como instrumento autorizativo de tratamento dos dados pessoais, à medida em que admite, sem impor condicionantes ou restrições nítidas, outras bases autorizativas para o tratamento dos referidos dados, tais como o cumprimento de obrigação legal ou regulatória pelo controlador; (...) Oferta-se, assim, um indesejável e potencialmente lesivo apequenamento do consentimento em face de outras bases autorizativas, de modo que não será estranho notar que os agentes de tratamento de dados sequer necessitam ou prefiram obter o consentimento do usuário (BASTOS et al, 2021, p.29260).

Além disso, no que concerne aos dados de saúde, também é importante notar, como levantado por Machado e Tavares (2023), que a legislação não estabelece um modelo específico para classificar os dados de saúde com base em sua sensibilidade, tampouco desenvolve sobre quais profissionais e serviços podem acessar esses dados ou como o compartilhamento das informações deve ser conduzido.

Já a Estratégia Brasileira para Transformação Digital (E-Digital), publicada em 2018, visa estimular a soberania digital por meio do fortalecimento da segurança cibernética, criação

de ambientes digitais seguros e a promoção da inovação tecnológica (BRASIL, 2018). Além disso, busca promover a interoperabilidade de sistemas de informação, a simplificação e digitalização de serviços públicos e a proteção de dados pessoais, considerando, conforme destacado nas políticas apresentadas acima, a importância da privacidade e da segurança das informações (BRASIL, 2018). Nesta estratégia, podemos dar destaque ao reconhecimento da "necessidade de atualizar o marco normativo incidente sobre o ambiente digital" (BARRIOS, Lucas, 2023, p.27), considerando, também, estratégica a construção de centros de dados no Brasil. Tal política foi deixada de lado no MCI; ela tem o objetivo de favorecer o desenvolvimento nacional e proporcionar maior segurança, reconhecida a desvantagem de depender excessivamente de serviços oferecidos por empresas estrangeiras, como serviços de internet e armazenamento em seus centros de dados (BRASIL, 2018, p.65).

De todo modo, embora as políticas acima representem grandes avanços no que concerne à proteção de dados pessoais da população brasileira, e ainda estejam em estágio inicial de implementação, haja vista que a LGPD, por exemplo, somente começou a vigorar em setembro de 2020, não é possível afirmar que elas hoje são capazes de combater as práticas extrativistas realizadas pelos monopólios informacionais, como o dataísmo e o colonialismo de dados. Isto pois, como mencionado anteriormente, o tipo de dominação que vem ocorrendo na esfera digital ocorre também no mundo material, físico, por meio do controle das tecnologias e suas infraestruturas, dos dados e as ferramentas que os coletam, criando uma situação de dependência crônica e estrutural.

Ainda que a construção de centros de dados em solo brasileiro seja urgente e essencial, a atual arquitetura global nos coloca numa situação em que, mesmo que os dados sejam armazenados no Brasil, eles ainda precisam trafegar por infraestruturas que passam por outros países, em especial os EUA, fazendo com que os dados permaneçam vulneráveis a interceptação e vigilância (BEZERRA e WALTZ, 2014). Tal cenário reduz a eficácia dessas medidas normativas, que ainda são pensadas e voltadas para operar em sistema econômico mundial que favorece o capitalismo de vigilância.

Além disso, compartilhar dados e informações sensíveis se tornou um movimento involuntário na prestação e contratação de serviços. Quem os contrata, seja um órgão governamental, empresa ou cidadão, se vê obrigado a aceitar termos de uso e compromisso e, caso não os aceite, é obrigado a recorrer a outras alternativas, geralmente mais caras, de difícil acesso ou menos eficientes. Cada vez mais o cotidiano está rodeado de interações, intencionais ou não, com essas tecnologias digitais. Por meio de celulares, relógios inteligentes, cartões de crédito, câmeras, etc, informações pessoais, senhas, dados bancários,

registros de ida e vinda de estabelecimentos, horário de despertar, dormir, frequência de atividades físicas e outros comportamentos que nem acreditamos poderem ser quantificados, deixam rastros, que são detectados e armazenados pelas redes.

Infelizmente, dependemos, nos mais diferentes níveis, desses cadastros e registros para utilizarmos ferramentas indispensáveis para trabalho, estudo e comunicação em nosso dia a dia. Portanto, não é estranho e nem mesmo incomum o sentimento de aprisionamento no mundo 'dataísta', posto que, quando começamos a refletir sobre a arquitetura que permeia o mundo digitalizado, compreendermos que ela foi projetada para atender aos interesses das grandes empresas, assim como nos manter reféns, física e psicologicamente, de seus produtos.

Em síntese, embora as políticas acima busquem reforçar a capacidade do Estado de exercer sua soberania no espaço virtual, e representem um importante estágio inicial para sua consolidação, elas não são suficientes, posto que carecem de diálogo entre si e não deixam claro como se dará continuidade às suas iniciativas por meio de outras políticas voltadas a proteção de dados pessoais e produção de tecnologias verdadeiramente nacionais (BARRIOS, 2023) - o que mantém país refém destas tecnologias estrangeiras e as consequências dessa externalização de serviços.

Exemplo desta fragilidade em que se encontram as políticas digitais no Brasil pôde ser constatada com o ataque sofrido pelo Ministério da Saúde em dezembro de 2021. Nesta ocasião, conforme noticiado pelo jornal G1, o ambiente virtual em que se encontra a nuvem pública de Saúde do MS, armazenada e processada pela empresa estrangeira Amazon, foi alvo de ataques cibernético (G1, 2021), onde "os hackers conseguiram entrar na nuvem dos arquivos e excluir os sistemas de ambiente virtual, além de deletar dados sobre vacinas, registros de casos e de óbitos relacionados à pandemia de covid-19" (MARGI, 2022, p.1). Deste modo, informações importantíssimas para administração pública foram transgredidas, afetando o desenvolvimento de políticas públicas voltadas à saúde.

Consequentemente, é possível compreender que a externalização de serviços de tecnologia chave da administração pública federal para empresas estrangeiras, como os serviços de armazenamento em nuvem, suscetíveis aos interesses dessas companhias e submetidos a legislações estrangeiras, escancaram as facetas do colonialismo digital, podendo levar à perda e controle sobre dados críticos para a saúde pública, comprometendo a soberania nacional.

Pois bem, mas o que a Amazon tem a ver com isso? Como mencionado, no que diz respeito aos serviços de armazenamento, além de ser a mais acionada mundialmente, a Amazon tem sido a empresa mais requisitada pelos órgãos federais brasileiros para prestação

de serviços de nuvem, sendo responsável pelo armazenamento e processamento de dados sensíveis da população, em especial no setor de saúde. Desde 2019, os dados pertencentes ao Ministério da Saúde são armazenados e processados nos servidores da AWS. Portanto, o próximo capítulo busca discutir os riscos da contratação da multinacional estrangeira, provedora de serviços de armazenamento e processamento de dados em nuvem para o Ministério da Saúde, para o campo da saúde pública no Brasil.

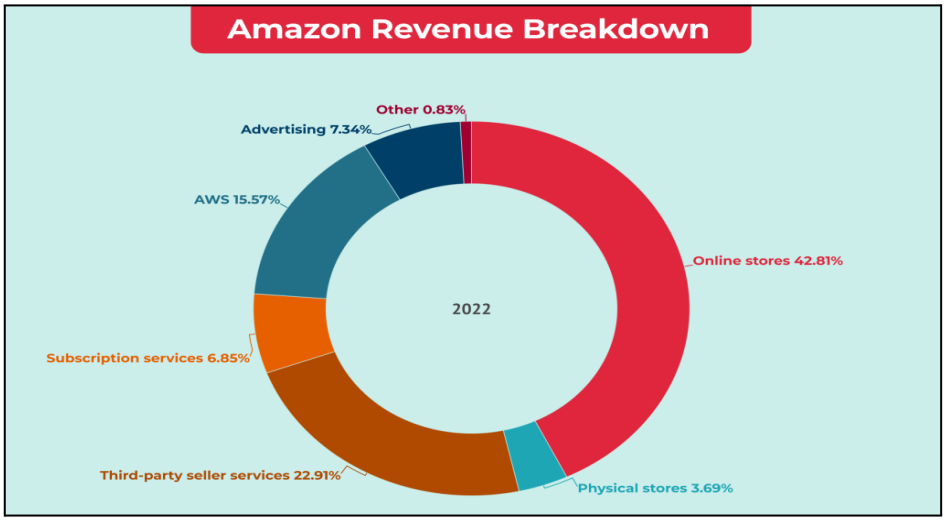
4 - Amazon e os riscos para o Brasil

4.1 - O que é a Amazon e qual sua relação com o setor de saúde?

A Amazon é uma empresa estadunidense que possui atuação global, presente nas áreas de comércio eletrônico, marketing digital, computação em nuvem, inteligência artificial e, embora mais recente, também no campo da saúde (AMAZON, 2022a). Pertencente ao grupo das *Big Five*, as cinco maiores empresas de tecnologia no mundo, logrou, no primeiro semestre de 2023, de acordo com a *Companies Market Cap* (2023) – site que monitora e disponibiliza online, de maneira atualizada, a lista das companhias mais valiosas em escala global –, a quinta posição no ranking das empresas com maior valor de mercado, com a impressionante marca de US$1.290 trilhões, com receita anual de cerca de US$500 bilhões em 2022 (CMC, 2023; STATISTA, 2023).

Como é possível observar na figura abaixo, elaborada por Cuofano (2023) tendo como base o 'Relatório Anual da Amazon de 2022', a receita da empresa parte principalmente de três segmentos, sendo eles: (i) comércio eletrônico, representando mais de 40% de receita da companhia; (ii) serviços de vendedores terceirizados, pessoas físicas ou jurídicas que utilizam da plataforma como ambiente para vender diretamente aos compradores, com mais de 20% e, por fim; (iii) a Amazon Web Services, também conhecido como AWS, que diz respeito ao segmento da empresa que desenvolve e comercializa tecnologias de infraestrutura, como computação em nuvem, armazenamento e bancos de dados, representando cerca de 15% da receita (AMAZON, 2022a; CUOFANO, 2023).

Figura 07: Detalhamento da receita da Amazon



Fonte: CUOFANO, 2023.

Embora não seja o maior, este último é o segmento que tem gerado maior lucro para a companhia - já em 2019 a AWS correspondeu a 70% do lucro total, em seu último trimestre (BBC, 2019). Em 2022, este segmento foi capaz de gerar cerca de US$23 bilhões em receita operacional e, finalmente, de acordo com dados do quarto trimestre do mesmo ano, a empresa manteve-se como principal fornecedor de serviços de infraestrutura em nuvem em escala global, com 32% de todo o mercado (CUOFANO, 2023; STATISTA, 2023).

À vista disso, diversas companhias de tecnologia, e principalmente a Amazon, têm buscado explorar e expandir suas operações para outros campos, dentre eles o setor de saúde - movimento esse relativamente recente e intensificado pela pandemia da Covid-19, que amplificou o papel dos serviços digitais (OZALP et al, 2022). Consequentemente, frente ao desenvolvimento das tecnologias 4.0, compreendidas como ferramentas 'inteligentes' – mecanismos que se comunicam via internet utilizando-se de armazenamento em nuvem e inteligência artificial, possibilitando troca de informações de maneira autônoma (SANTOS et al, 2018) – surgem novas alternativas para coleta e armazenamento de informações. Assim, as *Big Techs* avançam para suprir déficits relacionados aos serviços de atendimento em saúde e até mesmo de equipamentos hospitalares, aplicando essas novas tecnologias, que se comunicam por aplicativos móveis e *wearables,* como ferramentas digitais de monitoramento de saúde e relógios inteligentes, para ocupar espaço no tratamento dos dados sensíveis recolhidos, visando crescimento baseado na digitalização (FIOCRUZ, 2023a).

Por exemplo, na área clínica, a empresa vem desenvolvendo a *Amazon Comprehend Medical*, inteligência artificial capaz de analisar e extrair informações de receitas, anotações, relatórios e diagnósticos médicos em enormes quantidades para automatizar processos, oferecer soluções para firmas, automatizar testes clínicos e desenvolver perfis de pacientes (GUZMAN et al, 2019). De igual modo, por meio de assistentes virtuais, alimentadas com os dados extraídos pelas mais diversas ferramentas da Amazon, como a tecnologia ALEXA – inteligência artificial controlada por voz –, já é possível tirar dúvidas sobre determinados procedimentos médicos, pesquisar sobre sintomas de doenças e, utilizando somente comandos de voz, comprar medicamentos disponibilizados no site da companhia.

Inclusive, de acordo com Andy Jassy, CEO da empresa, adentrar e explorar o setor de atenção primária à saúde faz parte dos objetivos da empresa, considerado uma de suas próximas fronteiras (PRINGLE, 2023). A Amazon tem buscado expandir sua atuação no setor de saúde desde 2018. Primeiramente, adquiriu lojas de venda online de fármacos, como a *PillPack*, e provedoras de serviços médicos, como a *One Medical*, ao mesmo tempo em que vem desenvolvendo dispositivos inteligentes – como a Amazon Halo, pulseira rastreadora de

saúde e condicionamento físico – para monitorar e fornecer aos consumidores informações sobre sua saúde (LERMAN e SHABAN, 2022). Não obstante, a divisão de serviços em nuvem *Amazon Web Services* também tem buscado oferecer soluções específicas para o setor de saúde, como a *Amazon Health Lake*, ferramenta voltada à análise de dados para diagnósticos e tratamentos (LERMAN e SHABAN, 2022).

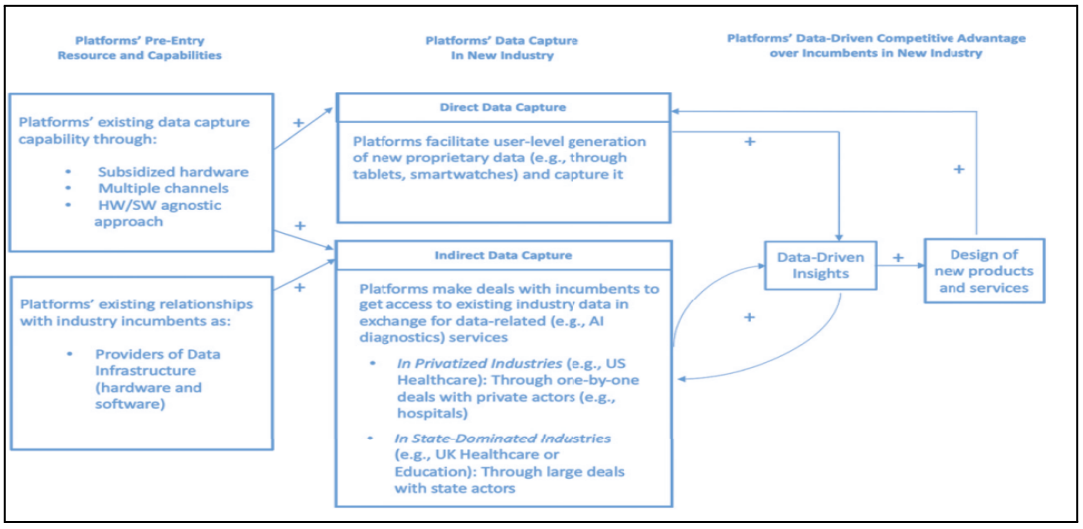
Observa-se que a multinacional está direcionando esforços para se envolver diretamente com os consumidores nessa área, e tem utilizado seus serviços de armazenamento, compra e venda online, monitoramento, análise em tempo real e dispositivos inteligentes para se estabelecer no campo da saúde. Logo, quais são as consequências da contratação da multinacional estrangeira Amazon - atual provedora de serviços de armazenamento e processamento de dados em nuvem para o Ministério da Saúde - para saúde pública no Brasil?

4.2 - *Big Techs* em setores altamente regulados

Primeiramente, cabe ressaltar que a escolha da *Amazon Web Services* como empresa responsável pela plataforma de armazenamento de dados de saúde do SUS foi feita sem um processo transparente de seleção pública, sem consulta à sociedade civil e aos órgãos de controle e, já em 2020, profissionais da área de tecnologia enxergavam seu processo de licitação como um risco à soberania digital brasileira (MOTORYN, 2022).

De acordo com Ozalp et al (2022), conforme exemplificado na figura abaixo, é possível observar um padrão na maneira pela qual essas grandes companhias adentram os setores historicamente mais regulados, como o da saúde.

Figura 08: Processo de entrada de *Big Techs* em setores altamente regulamentados.



Fonte: OZALP et al, 2022, p.97.

Primeiramente, iniciam-se como fornecedoras de serviços de infraestrutura de dados, como as nuvens de armazenamento. Em seguida, consolidam sua participação no setor utilizando seus recursos de análise e ferramentas mais avançadas e exclusivas do mercado – como a própria AWS, para processar dados e gerar resultados com suas tecnologias de Inteligência Artificial e *machine learning* – a partir das informações compartilhadas pelos prestadores de serviços que as contratam, sejam estes empresas ou governos. Por fim, tornam-se as provedoras exclusivas das informações orientadas por esses dados sensíveis, como diagnósticos e relatórios, e desenvolvem novos produtos e serviços – tais como o *Amazon Health Lake*, voltados justamente para analisar dados de saúde, produzindo modelos que possam prever e oferecer diagnósticos – com objetivo de oferecer soluções para empresas e governos.

Argumento que essas são características do colonialismo digital que podem ser aplicadas na contratação da AWS como nuvem pública do Ministério da Saúde no Brasil, onde, a partir desta decisão, podemos observar: (i) transferência de recursos, (ii) crescente dependência tecnológica e (iii) risco a perda de soberania sobre os dados. Pontos esses que receberão maior atenção na próxima seção.

Bem como alertado por Rachid et al (2023), a atuação dessas empresas pode ser caracterizada a partir de três elementos essenciais: primeiramente, elas têm buscado coletar e armazenar uma quantidade cada vez maior de dados sobre seus usuários/consumidores; esses dados são considerados recursos e ativos econômicos, visto que, a partir deles, conseguem otimizar sua oferta de serviços. Segundo, a partir dessa coleta, buscam construir bases de usuários/consumidores cada vez maiores, de maneira a potencializar geração de receitas através de publicidade, vendas diretas e outras formas de monetização. Por fim, utilizam de um contexto de crescente financeirização para ampliar seus negócios e investir em outras áreas além de sua atividade principal, também se beneficiando da coleta de dados e da construção de grandes bases de usuários para impulsionar seus negócios (RACHID et al, 2023).

4.3 – Riscos da contratação da Amazon

Assim, tendo em vista a literatura levantada neste trabalho, é possível compreender que a contratação dos serviços de armazenamento em nuvem da Amazon para a administração

pública federal, como o Ministério da Saúde, pode agravar vulnerabilidades em relação à segurança e privacidade dos dados de saúde dos brasileiros, posto que, conforme discutido, as atuais políticas brasileiras não são capazes de combater as práticas extrativistas realizadas pelos monopólios informacionais, e também não se vê tendência a ampliar esta discussão para a sociedade civil. Consequentemente, representa fomento à crescente dependência tecnológica, subordinação a interesses estrangeiros e acesso aos dados privados, características do colonialismo digital.

Ao serem alimentadas e treinadas com os dados e informações dos milhões de usuários que utilizam suas plataformas, as ferramentas de análise da Amazon aprimoram-se, em um patamar nunca antes visto, para desenvolver e oferecer novos produtos e serviços cada vez mais personalizados e únicos. A partir daí, estabelecem as novas fronteiras das tecnologias digitais e dominam o mercado, aprofundando as desigualdades e barreiras de entrada já presentes no setor.

A dependência também está presente na esfera "produtiva e tecnológica do exterior, sobretudo em segmentos de fármacos e de equipamentos médico-hospitalares" (FIOCRUZ, 2023, p. 109), afetando, inclusive, "a capacidade inovativa" brasileira. Isto pois, conforme alertado por José Mauro da Conceição Pinto, professor e pesquisador da Escola Politécnica de Saúde Joaquim Venâncio (EPSJV/Fiocruz), em entrevista disponibilizada pela Fiocruz, o avanço da lógica neoliberal sobre o Complexo Econômico-Industrial da Saúde brasileiro caminha em paralelo a um processo de desvalorização do setor de informática do SUS (ANTUNES, 2020). Como reforça José Mauro, são poucas as iniciativas de desenvolvimento e produção de conhecimento nacional, e é normalmente dada preferência à terceirização:

> contratam empresas que desenvolvem softwares e são elas que desenvolvem produtos com a chancela DataSUS. Tudo bem: tem um termo de confidencialidade. O que proíbe ele de depois fazer um software que use aquelas funcionalidades para vender no mercado? (PINTO, José, 2020; apud ANTUNES, 2020).

Assim, pode acabar por acentuar as desigualdades de acesso da população aos serviços públicos de saúde, posto que, somando-se a concentração de recursos financeiros no mercado privado de planos de saúde, que também já possui acesso a uma quantidade maior de leitos (NAVARRETE, 2017), vem a tornar-se possível entrave adicional à consolidação da universalização do SUS. Pois,

> ao contribuir com elevação de gastos privados, cuja proporção já é maior que a de gastos públicos na saúde no Brasil, o capital estrangeiro pode drenar serviços, recursos humanos e financeiros do SUS, constituindo-se em mais um vetor de desigualdades de acesso da população à assistência em saúde (SCHEFFER e SOUZA, 2022, p.9).

Vale ressaltar que a Amazon já foi processada por supostamente violar as leis de proteção de dados da União Europeia (UE), além de utilizar os dados sobre a atividade de vendedores terceirizados em sua plataforma (BBC, 2021), abusando de sua predominância no mercado para obter uma vantagem injusta sobre concorrentes. Nesta ocasião, conforme apresentado pela BBC (2021), a Comissão Nacional de Proteção de Dados de Luxemburgo argumentou que a empresa não estava seguindo a legislação da UE, somando-se, inclusive, ao risco desses dados serem explorados para fins comerciais pela AWS ou outras empresas parceiras, assim como treinamento de IA.

Portanto, no campo da saúde, com sua abertura ao capital privado - haja vista o que vem sendo desenvolvido com as políticas brasileiras de saúde digital - e a participação cada vez maior de empresas estrangeiras em setores estratégicos para o país, o Estado brasileiro vem se colocando numa posição de risco. Como alertado por Vera Guasso (2020), diretora do Sindicato dos Trabalhadores em Processamento de Dados do Rio Grande do Sul, este movimento representa uma "perda acelerada de soberania do país e ao mesmo tempo um risco gigantesco, porque essas empresas têm compromissos de passar informações para os governos (estrangeiros), por exemplo.".

Desta forma, observa-se na contratação da multinacional estrangeira Amazon como provedora de serviços de armazenamento e processamento de dados em nuvem para o Ministério da Saúde um exemplo claro da dinâmica narrada no capítulo anterior sobre o funcionamento da economia de dados. Trata-se de uma manifestação da lógica neoliberal: partindo da dificuldade de tratar os dados das empresas e da sociedade no próprio território e em instituições nacionais, somando a transferência de recursos para o setor privado, que opera em benefício da manutenção da dependência das tecnologias estrangeiras, temos um circuito de colonialidade bastante preocupante ao SUS e sua prestação de serviços físicos também.

No que diz respeito a transferência de recursos, com a contratação da AWS, intermediada pela Embratel a partir do Edital nº 29/2018 "Serviços de computação em nuvem", é possível observar a transferência de recursos do Brasil para o exterior – infelizmente, as informações deste contrato não estão disponíveis para o público. De igual modo, embora a Lei de Acesso à Informação tenha sido acionada, em trâmite de acordo com o processo legal n° 18870.004103/2022-89, referente ao contrato firmado entre o Serviço Federal de Processamento de Dados (Serpro)[5] – maior empresa pública brasileira de prestação

[5] Criado em 1964, o Serpro é responsável por armazenar informações sobre todos os cidadãos brasileiros, administrando o maior banco de dados do país. Além disso, é o principal provedor de soluções tecnológicas para o Estado. Frente a isso, mostra-se relevante comparar os valores dos contratos pois, no contexto da AWS, é

de serviços em tecnologia da informação – com a AWS, também não foi possível alcançar quebra de sigilo. Logo, não é possível, nem mesmo para efeitos de comparação, saber o valor exato dos contratos. Fica aqui o registro desta lacuna, que resulta de pesquisa empírica.

Conquanto a contratação da Amazon para prestação de serviços em nuvem não seja em si um problema, a utilização dessa infraestrutura, fornecida por uma empresa estrangeira, para armazenamento e processamento de dados sensíveis da população brasileira, essenciais para o desenvolvimento de políticas públicas por parte do MS, escancara os riscos de perda de soberania sobre a produção de tecnologia nacional e privacidade dos dados sensíveis da população.

Também, ao priorizar os serviços da Amazon, o Brasil está abrindo mão de sua capacidade de desenvolver, utilizar tecnologias próprias e de capacitar profissionais locais para atuar nessa área, fomentando conhecimento local e a produção de tecnologias intrinsecamente brasileiras. Isso acaba por atrasar, e até mesmo limitar a capacidade do país de desenvolver sua própria indústria de armazenamento em nuvem para a administração pública federal, afetando a geração de empregos e riqueza dentro do país.

À vista disso, observa-se que a administração pública neoliberal prioriza uma economia imediata, a terceirização e a confiança em contratos e, ao fazer isso, permitindo que cada vez mais as companhias assumam funções que anteriormente eram de responsabilidade do Estado, entregam à iniciativa privada a responsabilidade sobre a gestão de ativos como dados, softwares, patentes e tecnologias essenciais para a inovação, além de reduzir os investimentos estatais voltados para o desenvolvimento de tecnologias nacionais e capacitação profissional para sua manutenção. Colocando em jogo, portanto, uma disputa pelo conhecimento, inovação e capacidade de produzir tecnologias digitais verdadeiramente nacionais. Concomitantemente, como destacado na primeira seção do capítulo anterior, as empresas encontram benefícios nessa transferência de responsabilidade, promovendo seu ‘desempenho social positivo’ ao assumir este ‘fornecimento privado de bens públicos’, promovendo sua valorização no mercado e aumentando seu poder de barganha.

Outro ponto importante a ser destacado é que, ao analisarmos o “Contrato do cliente AWS”, contrato geral disponibilizado no site da Amazon e cuja última atualização ocorreu no dia 20 de janeiro de 2023, em sua primeira cláusula, denominada “Responsabilidade da AWS”, subseção 1.4, referente a privacidade dos dados, lê-se:

---

curioso como ela pode prestar serviços para MS e, ao mesmo tempo, estabelecer parceria com o Serpro através de outro contrato, possivelmente com diferentes preços, que abrange as mesmas atividades para o mesmo ministério (QUEIROZ, 2022).

> (...) A AWS não acessará nem usará o seu conteúdo, exceto se necessário para manter ou estabelecer os serviços, ou caso seja necessário para cumprir com as leis ou uma ordem vinculativa emitida por autoridades governamentais. Nós não (a) divulgaremos o Seu Conteúdo para quaisquer governos ou terceiros; ou (b) transferiremos o Seu Conteúdo das regiões AWS selecionadas por você, exceto se, em cada caso, assim for necessário para cumprir com as leis ou com uma ordem vinculativa emitida por quaisquer autoridades governamentais. (AMAZON, 2022b, p.3).

Observa-se que nele pouco é desenvolvido acerca do que vem a ser o necessário para manutenção dos serviços prestados, posto que, na função de armazenadora e processadora dos dados, compreende-se que a Amazon precisa ter algum tipo de acesso a essas informações. Logo, quais são essas necessidades mencionadas no contrato: do governo brasileiro ou da própria Amazon?

De igual modo, no que diz respeito ao compartilhamento desses dados para cumprir com leis ou ordem vinculativa, vale ressaltar que nos Estados Unidos as empresas estão submetidas ao *Communications Assistance for Law Enforcement Act* (CALEA), mecanismo legal que facilita a vigilância eletrônica. De acordo com esta Lei, operadoras e fabricantes norte-americanas de equipamentos de telecomunicações precisam desenvolver seus equipamentos e serviços de maneira a garantir a presença de recursos de vigilância necessários para atender a solicitações legais de informações (FCC, 2023), o que pode tornar vulneráveis todos os dados de um país que contrate serviços de armazenamento destas empresas.

Frente a isso, a crescente participação de empresas, nacionais e estrangeiras, na área da saúde, somada à coleta massiva de dados por órgãos públicos, torna necessário maior atenção à segurança cibernética para proteger os direitos dos cidadãos, especialmente com o uso destas tecnologias emergentes, como Inteligências Artificiais e Internet das Coisas, que podem tornar opaco o processamento de dados e as decisões tomadas tendo eles como base (UNCDF, 2021; NIC, 2023).

Isto pois, "alguns tipos de decisões algorítmicas escapam às leis atuais, principalmente aquelas originárias de algoritmos complexos com capacidade de causar exclusões silenciosas, difíceis de serem comprovadas na esfera judicial" (SOUZA, Delton, 2022, p.23).

Ao tomarmos como base o *Global Cybersecurity Index* (2022/23), estudo realizado pelo Instituto de Tecnologia de *Massachusetts* (MIT), que avalia o nível de segurança cibernética das vinte maiores economias do mundo, é possível observar que o Brasil encontra-se na décima oitava posição no ranking, à frente somente de Turquia e Indonésia.

Portanto, quando comparado a outras grandes potências econômicas, ainda está iniciando no processo de tornar-se resiliente frente às ameaças digitais, buscando desenvolver medidas legais, técnicas e organizacionais para incidir sobre esta problemática.

Logo, também cabe analisar justamente o impacto da crescente utilização de ferramentas de Inteligência Artificial na saúde. No Brasil, ela já faz parte de políticas como o Conecte SUS e a RNDS, apresentadas anteriormente, que utilizam da tecnologia para ampliar a oferta de serviços de saúde, aprimorar atendimentos e promover diagnósticos mais assertivos. Porém, conforme elencado por Lima (2022), os grandes desafios e riscos para sua implementação residem em garantir que sua utilização seja justa e não discriminatória.

Isto pois, segundo o autor, mesmo que o desenvolvimento de determinada IA, voltada para a melhoria dos serviços de saúde, ocorra de maneira precisa, ou seja, não existam erros em sua programação e ela se apresente capaz de analisar e interpretar os dados que a alimentam, esta ferramenta ainda estará suscetível aos dados enviesados que está recebendo. De igual modo, também está suscetível a falhas na sua própria estrutura, o que "pode levar a um efeito de amplificação ou perpetuação de tratamentos discriminatórios, problema agravado pela falta de transparência em alguns modelos" (LIMA, Jefferson, 2022, p.38).

Assim, ao serem capazes de analisar somente os dados que são fornecidos, sejam estes de boa qualidade ou não, as IA carecem da capacidade de interpretá-los em diferentes contextos, o que pode ofuscar informações importantes para o resultado final, limitando sua análise e abrindo espaço para a generalização dos resultados. Por exemplo, conforme observado por Obermeyer et al (2019), foi possível constatar indícios de discriminação racial em um algoritmo amplamente utilizado no sistema de saúde dos EUA para estratégias em saúde. Neste caso, a ferramenta, ao considerar em suas análises 'gastos em saúde' como um indicador de necessidades médicas, acabou por reduzir em mais da metade em seus resultados o número de pacientes negros identificados para receber cuidados suplementares. Refletindo, portanto, um problema estrutural presente nos EUA, onde pacientes negros com a mesma necessidade de cuidados do que pacientes brancos acabam recebendo menos recursos financeiros, levando o algoritmo a erroneamente concluir que pacientes negros estão em um estado de saúde melhor e, portanto, não se classificariam para receber esses cuidados suplementares (OBERMEYER et al, 2019).

Portanto, para o setor da saúde do Brasil, torna-se de suma importância que o desenvolvimento e implementação dessas novas tecnologias priorizem os princípios básicos do SUS de universalização e equidade. A partir daí, há o questionamento: como podemos

garantir que as tecnologias de IA produzidas pela Amazon, utilizadas para o processamento de informações da RNDS, estão adequadas aos princípios fundamentais do SUS?

5 - Conclusão

Tendo em vista os argumentos apresentados e discutidos neste trabalho, é possível observar que, cada vez mais, a responsabilidade sobre provisão de serviços públicos tem sido transferida do governo para o setor privado, como discutido sobre o caso da saúde pública brasileira. Concomitantemente, frente a tendência a 'plataformização' das infraestruturas públicas e privadas, compartilhar dados e informações sensíveis se tornou algo involuntário, posto que estamos aprisionados em interações, intencionais ou não, com máquinas e ferramentas digitais programadas para a todo momento aprender mais sobre como nos comportamos. Com esse processo, vivemos sob constante vigilância, não há espaço para privacidade, e nos tornamos, portanto, mercadoria a ser explorada, reféns dos monopólios informacionais.

Na rua, no mercado, no shopping, nas praias, nas academias, nas universidades etc, há um constante monitoramento, seja pelos aparelhos eletrônicos que carregamos, pelas câmeras de monitoramento espalhadas, sensores e satélites. Com isso, observa-se que quem nasce no mundo digital será, de alguma maneira, capturado e contabilizado pelos sistemas de dados, sem que possa opinar sobre essa decisão. Portanto, cabe o questionamento: como podemos falar sobre o 'direito de ser deixado de lado'? Como podemos deixar de ser reféns desses sistemas se eles próprios foram construídos para que não possamos fugir? Agora, com o mundo digitalizado, a matéria prima somos nós, nossos dados, rastros, interações, pensamentos; nos tornamos as *commodities* dessas grandes empresas.

Somado a esta questão, que envolve a própria dinâmica de funcionamento do sistema econômico mundial, está o fato de que o cidadão brasileiro não está pronto para essas tecnologias que nos são impostas. Não possuímos segurança cibernética efetiva, letramento ou consciência digital. De igual modo, não é comum que os usuários leiam por completo os termos de uso e política de privacidade destas ferramentas e, mesmo que tentem, irão se deparar com documentos com centenas de páginas, repletos de jargões jurídicos, buscando dificultar ao máximo sua compreensão. O próprio sistema é feito para que não possamos descobrir o que está em jogo.

Ademais, o problema também está na carência de políticas públicas e debates para abordar a questão - raros são os espaços de deliberação democrática para tratar de assuntos como a proteção de dados sensíveis e a busca pela autonomia e soberania tecnológica brasileira. Quando estes espaços existem, a exemplo do 'Seminário sobre Saúde Digital' – evento ocorrido em abril de 2023, promovido pelo Conselho Nacional de Saúde (CNS) com o

apoio da Fiocruz, no intuito de discutir, por exemplo, a utilização de tecnologias de comunicação, informação e coleta de dados no campo da saúde –, pouco são divulgados e limitam a participação da sociedade civil, deixando nas mãos de poucos decisões e debates que dizem respeito a toda uma nação.

Conforme discutido, no campo da saúde, com sua abertura ao capital privado - haja vista o que vem sendo desenvolvido com as políticas brasileiras de saúde digital - e a participação cada vez maior de empresas estrangeiras em setores estratégicos para o país, o Estado brasileiro vem se colocando numa posição de risco. Embora o DataSUS e a RNDS sejam iniciativas inovadoras que certamente oferecem benefícios para os cidadãos brasileiros, elas trazem consigo a dependência dos serviços de processamento de dados e armazenamento em nuvem da Amazon, que por sua vez não carregam em sua arquitetura os princípios básicos do SUS de universalização e equidade. Refletindo, também, as dinâmicas narradas neste trabalho sobre o colonialismo digital, tornando-se, portanto, prejudicial para o SUS e, consequentemente, para o Brasil.

Portanto, para que um novo cenário seja possível, é necessário repensar a maneira como estas tecnologias são produzidas, repensar a arquitetura jurídica, nacional e internacional, assim como reformular o ensino básico e superior para nos preparar para interagir com o mundo digital de maneira mais comunitária. Também, é preciso ampliar discussões que debatam a ética das empresas, de maneira a impor responsabilizações que realmente sejam efetivas, além de fomentar, a exemplo do Plan CEIBAL e do Programa de Emergência para a Soberania Digital brasileira, alternativas que fujam da atual lógica neoliberal e suas ameaças, sendo capazes de incentivar a autonomia dos países em desenvolvimento e suas populações a superar as desigualdades e dependências perpetuadas pelo colonialismo de dados.

6 - Referências Bibliográficas

ALMEIDA, Luciene. **Regulamentação da telemedicina impacta a formação médica e expõe desafios que ultrapassam a tecnologia.** Site da internet, 2023. Disponível em <https://newslab.com.br/regulamentacao-da-telemedicina-impacta-a-formacao-medica-e-expoe-desafios-que-ultrapassam-a-tecnologia/> Acesso em: maio de 2023.

AMADEU, Sergio. **A hipótese do colonialismo de dados e o neoliberalismo.** In: AMADEU, S., SOUZA, J., CASSINO, J. Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. Brasil: Autonomia Literária, 2021. p. 33-52. Acesso: junho de 2023.

AMADEU, Sergio. **Dataficação, vigilância e colonialismo de dados.** In: Simpósio Intersindical - Desafios Educacionais em Tempos de Pandemia. Dimensão Política-Tecnológica, [S. l.]: Apubh, 13 de ago. 2020. 1 vídeo (25 min: 12 seg). [Simpósio]. Disponível em: https://www.youtube.com/watch?v=JTpCNf-hb9Y. Acesso em: junho de 2023.

AMAZON, 2022a. ***Annual Report.*** Amazon, 31 de dezembro de 2022. Disponível em: <https://s2.q4cdn.com/299287126/files/doc_financials/2023/ar/Amazon-2022-Annual-Report.pdf>.Acesso em: março de 2023. Acesso em: maio de 2023.

AMAZON, 2022b. **Contrato de cliente (AWS).** Amazon, 25 de fevereiro de 2022. Disponível em: <https://d1.awsstatic.com/legal/aws-customer-agreement/AWS_Customer_Agreement_Portuguese_Translation1.pdf> Acesso em: março de 2023.

AMIOT et al. ***European Digital Sovereignty. Syncing Values and Value.*** Site da internet, 2020. Disponível em <https://www.oliverwyman.com/our-expertise/insights/2020/sep/european-digital-sovereignty.html>. Acesso em: maio de 2023.

ANTUNES, André. **Entrevista: José Mauro da Conceição Pinto.** Dezembro de 2020. Disponível em: <https://www.epsjv.fiocruz.br/noticias/entrevista/precisamos-rever-a-maneira-como-estamos-informatizando-o-sistema-de-saude-a>. Acesso em: maio de 2023.

ANTUNES, André. **Nova Política Nacional de Informação e Informática em Saúde suscita questionamentos de especialistas.** Brasil, 12 de agosto de 2021. Disponível em: <https://www.epsjv.fiocruz.br/noticias/reportagem/nova-politica-nacional-de-informacao-e-informatica-em-saude-suscita>. Acesso: junho de 2023.

ASSIS, Wendell. (2014). **Do colonialismo à colonialidade: expropriação territorial na periferia do capitalismo.** Caderno CRH, 27(72), 613–627. Disponível em: <https://doi.org/10.1590/S0103-49792014000300011>. Acesso: junho de 2023.

AVELINO, Rodolfo. **Colonialismo digital: dimensões da colonialidade nas grandes plataformas.** In: AMADEU, S., SOUZA, J., CASSINO, J. Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. Brasil: Autonomia Literária, 2021. p. 69-86. Acesso em: maio de 2023.

AVILA, Milena. **Colonialidade e Decolonialidade: você conhece esses conceitos?**. Brasil, junho de 2023. Disponível em: <https://www.politize.com.br/colonialidade-e-decolonialidade/>. Acesso: junho de 2023.

ASSIS, W. F. DO COLONIALISMO À COLONIALIDADE: **expropriação territorial na periferia do capitalismo.** Caderno CRH, [S. l.], v. 27, n. 72, 2015. DOI: 10.9771/ccrh.v27i72.19436. Disponível em: https://periodicos.ufba.br/index.php/crh/article/view/19436. Acesso em: julho de 2023.

AZEVEDO, V.; FERREIRA, V.; JUNIOR, C.; MARQUES, A.; OLIVEIRA, D.; PAGOTTO, D. **Inovação em saúde: A implementação de um data lake para o armazenamento, sistematização e disponibilização de dados em saúde no Brasil**. Universidade Federal de Goiás e a Secretaria de Gestão do Trabalho e da Educação na Saúde/Ministério da Saúde, 2022. Disponível em: <http://anpad.com.br/uploads/articles/120/approved/da0dba87d95286d836e37ca60ab1e734.pdf>. Acesso em: maio de 2023.

BAGUETE. **AWS: nuvem é uma política de estado no Brasil. Dezembro de 2022**. Disponível em <https://www.baguete.com.br/noticias/01/12/2022/aws-nuvem-e-uma-politica-de-estado-no-brasil>. Acesso em: maio de 2023.

BARON, D. P. (2009). ***A Positive Theory of Moral Management, Social Pressure, and Corporate Social Performance.*** Journal of Economics & Management Strategy, 18(1), 7–43. doi:10.1111/j.1530-9134.2009.00206.x. Acesso: junho de 2023.

BARRIOS, Lucas. **Soberania, Planejamento Estatal e Transformação Digital: análise comparada dos instrumentos jurídicos da União Europeia e do Brasil.** Rev. Seminário de Direito Econômico (2022). Acesso: junho de 2023.

BASTOS, E. A. V.; PANTOJA, T. L. S.; DOS SANTOS, S. H. C. S. **Os impactos das novas tecnologias da informação e comunicação no direito fundamental à privacidade / *The impacts of new information and communication technologies in the fundamental right to privacy.*** Brazilian Journal of Development, [S. l.], v. 7, n. 3, p. 29247–29267, 2021. DOI: 10.34117/bjdv7n3-578. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/26840. Acesso em: 29 jul. 2023. Acesso em: maio de 2023.

BBC. ***Amazon charged with abusing EU competition rules.*** Novembro de 2020. Disponível em <https://www.bbc.com/news/business-54887650>. Acesso em: maio de 2023.

BBC. ***Amazon hit with $886m fine for alleged data law breach.*** Julho de 2021. Disponível em <https://www.bbc.com/news/business-58024116>. Acesso em: maio de 2023.

BEZERRA, Arthur Coelho; WALTZ, Igor. **Privacidade, neutralidade e inimputabilidade da internet no Brasil: avanços e deficiências no projeto do marco civil**. Revista de Eletrônica Internacional de Economia Política da Informação da Comunicação e da Cultura, Florianópolis, v.16, n.2, p.157-171, maio/ago. 2014. Acesso em: maio de 2023.

BERNHAGEN, Patrick; MITHCELL, Neil. ***The Private Provision of Public Goods: Corporate Commitments and the United Nations Global Compact***. International Studies

Quarterly, 2010. 54. 1175 - 1187. 10.1111/j.1468-2478.2010.00631.x. Acesso em: maio de 2023.

BLUM, Renato e VAINZOF, Rony. **Conheça os pontos positivos e negativos do Marco Civil.** 2014. Disponível em <https://nic.br/noticia/na-midia/conheca-os-pontos-positivos-e-negativos-do-marco-civil/> Acesso: junho de 2023.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Diário Oficial, Brasília, 05 out. 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: maio de 2023.

BRASIL. **Controladoria-Geral da União (CGU). Lei de acesso à informação - recurso submetido à CGU parecer N° 54/2023/CGRAI/OGU/CGU.** Disponível em <https://www.gov.br/cgu/pt-br/assuntos/noticias/2023/02/mais-sete-recursos-sobre-sigilos-a-informacoes-publicas-sao-analisados-pela-cgu/parecer-4.pdf>. Acesso em: maio de 2023.

BRASIL. **Lei 8080 de 19 de setembro de 1990.** Diponível em <http://www.planalto.gov.br/ccivil_03/leis/l8080.htm>. Acesso em: maio de 2023.

BRASIL. **Lei 13.709 de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).** Diário Oficial da República Federativa do Brasil, 15 ago. 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/ L13709.htm. Acesso em: maio de 2023.

BRASIL. Ministério da Economia. **Estudo Técnico Preliminar - Processo administrativo nº 19973.100103/2020-51 - Aquisição centralizada de serviços de computação em nuvem.** Disponível em <https://sei.economia.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?dXxAxlDxfg5iXrvzdwJT8wIQgNYTeEkpDDNZSgrLzVmO4UFVESo97_WVDXtAZWjWgtDxRB6hKaEhst72j6o0fxKNssOBfKFL3cs4kHXOlROHTBI1bpObbkbLsyfvqGlg>. Acesso em: maio de 2023.

BRASIL. Ministério da Saúde. **DATASUS trajetória 1991-2002.** Secretaria-Executiva, Departamento de Informática do SUS - Brasília, DF, 2002. Acesso em: maio de 2023.

BRASIL. Ministério da Saúde. **Estratégia brasileira para a transformação digital (E-Digital**). Brasília, 2018. Acesso: junho de 2023.

BRASIL. Ministério da Saúde. **Estratégia de Saúde Digital para o Brasil 2020-2028.** Brasília, DF: Ministério, 2020. Disponível em <https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf> Acesso: junho de 2023.

BRASIL. Ministério da Saúde. **Plano de Ação, Monitoramento e Avaliação da Estratégia de Saúde Digital Para o Brasil 2019-2013**. Brasília, 2020. Disponível em <https://www.gov.br/saude/pt-br/assuntos/saude-digital/aestrategia-brasileira/PlanodeAoMonitoramentoeAvaliao.pdf> Acesso: junho de 2023.

BRASIL. Ministério da Saúde. **Estratégia Brasileira para a Transformação Digital.** Grupo de Trabalho Interministerial criado pela Portaria nº 842/2017. Documento Base para discussão pública. Brasília, DF, 2017.

BRASIL. Ministério da Saúde. **Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC: 2021-2024.** DATASUS, Companhia Nacional de Abastecimento. – Brasília, DF, 2021. Acesso em: maio de 2023.

BRASIL. Ministério da Saúde. **Política Nacional de Informação e Informática em Saúde.** Secretaria-Executiva, Departamento de Monitoramento e Avaliação do SUS. Brasília, DF, 2016. Acesso em: maio de 2023.

BRASIL, Ministério da Saúde. **Rede Nacional de Dados em Saúde - RNDS.** Disponível em <https://www.gov.br/saude/pt-br/composicao/seidigi/rnds> Acesso: junho de 2023

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> . Acesso em: maio de 2023.

BRASIL, Ministério da Saúde. **SUS: a saúde do Brasil**. Secretaria-Executiva, Subsecretaria de Assuntos Administrativos. – Brasília : Editora do Ministério da Saúde, 2011. Acesso: junho de 2023.

CARDOSO et al (2023). **Bolsonaristas invadem Congresso, Planalto e STF em manifestação antidemocrática**. Janeiro de 2023. Disponível em <https://www.metropoles.com/distrito-federal/bolsonaristas-extremistas-manifestacao-brasilia >. Acesso: junho de 2023.

CALGARO, Fernanda. **Governo recua e retira ponto sobre datacenters do texto do Marco Civil**. Site da internet, 2014. Disponível em <https://noticias.uol.com.br/politica/ultimas-noticias/2014/03/18/ministra-rebate-criticas-a-ponto-polemico-do-marco-civil.htm> Acesso em: julho de 2023.

CEGATTI et al (2020). **Terceirizações na área da saúde no Brasil: reflexos no SUS, nas políticas sociais e nos trabalhadores.** 12. 1-41. 10.14295/jmphc.v12.978. Acesso: junho de 2023

CETIC, Centro de Estudos sobre as Tecnologias da Informação e da Comunicação, 2021a. **Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro (2021)** Disponível em <https://cetic.br/media/docs/publicacoes/2/20220725170710/tic_governo_eletronico_2021_livro_eletronico.pdf> Acesso em: maio de 2023.

CETIC, Centro de Estudos sobre as Tecnologias da Informação e da Comunicação, 2021b. **TIC SAÚDE: Pesquisa sobre o Uso das Tecnologias De Informação e Comunicação nos Estabelecimentos de Saúde Brasileiros (2021).** Disponível em: https://cetic.br/media/docs/publicacoes/2/20211130124545/tic_saude_2021_livroeletronico.pdf> Acesso em julho de 2023.

CMC, Companies Market Cap. ***Largest Companies by Market Cap.*** Site da internet, 2023. Disponível em <https://companiesmarketcap.com>. Acesso em: julho de 2023.

COELHO NETO, Giliate C.; CHIORO, Arthur. **Afinal, quantos Sistemas de Informação em Saúde de base nacional existem no Brasil?.** Cadernos de Saúde Pública, Rio de Janeiro, v. 37, n. 7, p. e00182119, 2021. Disponível em < https://doi.org/10.1590/0102-311X00182119>

CUOFANO, Genaro. **Amazon Revenue Breakdown**. Junho de 2023. Disponível em <https://fourweekmba.com/amazon-revenue-breakdown/>

CUNHA, Elenice Machado da; VARGENS, José Muniz da Costa. **Sistemas de informação do Sistema Único de Saúde**. In: GONDIM, Grácia Maria de Miranda; CHRISTÓFARO, Maria Auxiliadora Córdova; MIYASHIRO, Gladys Miyashiro (Org.). Técnico de vigilância em saúde: fundamentos. v. 2. Rio de Janeiro: EPSJV, 2017. p. 71-112

DERIVRY, Tamian. ***Digital Sovereignty in India: Policy agenda, discourse, power and capability.*** SciencesPo, 2023. Disponível em <https://www.sciencespo.fr/public/chaire-numerique/en/2023/05/04/contribution-digital-sovereignty-in-india-policy-agenda-discourse-power-and-capability/> Acesso: junho de 2023.

DIOGENS, Maria; RIBEIRO, Maria. **Avaliação de Tecnologias em Saúde.** Jornal Tribuna, 2023. Disponível em <https://jornaltribuna.com.br/wp-content/uploads/2023/03/ARTIGO-Avaliacao-de-Tecnologia-em-Saude.pdf>. Acesso: junho de 2023.

DUARTE, Pedro e GACIOLLI, Edílson**. A Teoria da dependência: interpretações sobre o (sub)desenvolvimento na América Latina**. UNICAMP, 2017.

EPSTEIN, Robert. **The new mind control: The internet has spawned subtle forms of influence that can flip elections and manipulate everything we say, think and do**. Fevereiro de 2016. Disponível em <https://aeon.co/essays/how-the-internet-flips-elections-and-alters-our-thoughts>

EVANGELISTA, Rafael. **Programa de emergência para a soberania digital**. Site da internet, 18 Agosto 2022. Disponível em <https://www.ihu.unisinos.br/categorias/621347-programa-de-emergencia-para-a-soberania-digital>. Acesso em: julho de 2023.

FARIA, Manuel; NOBRE, Victor. **O Orçamento da Saúde para 2023: o que mudou nos últimos dez anos?.** Instituto de Estudos para Políticas de Saúde (IEPS), 2023. Disponível em <https://ieps.org.br/wp-content/uploads/2023/04/IEPS_NT29.pdf>. Acesso: junho de 2023.

FARIA, Manuel; NOBRE, Victor; TASCA, Renato; AGUILLAR, Arthur. **A Proposta de Orçamento para Saúde em 2022.** Instituto de Estudos para Políticas de Saúde (IEPS), 2023. Disponível em <https://static.poder360.com.br/2021/11/IEPS-nota-tecnica-ploa-2022.pdf>. Acesso em: julho de 2023.

FCC. Federal Communications Commission. **Communications Assistance for Law Enforcement Act (CALEA).** Julho de 2023. Disponível em <https://www.fcc.gov/calea#:~:text=The%20Communications%20Assistance%20for%20law,necessary%20surveillance%20capabilities%20to%20comply>. Acesso em: julho de 2023.

FIOCRUZ. **Proteção de Dados Pessoais em Serviços de Saúde Digital no Brasil.** Março de 2023. Disponível em

<https://intervozes.org.br/publicacoes/resumo-executivo-protecao-de-dados-pessoais-em-servicos-de-saude-digital-no-brasil/> . Acesso em: maio de 2023.

FIOCRUZ, Ministério da Saúde. **Saúde é desenvolvimento: o Complexo Econômico-Industrial da Saúde como opção estratégica nacional'**. Centro de Estudos Estratégicos da Fiocruz Antonio Ivo de Carvalho. Rio de Janeiro, 2022. Disponível em <https://cee.fiocruz.br/?q=node/1660>. Acesso em: maio de 2023.

FIOCRUZ, Ministério da Saúde. **Universalidade.** Disponível em <https://pensesus.fiocruz.br/universalidade#:~:text=Universalidade%20é%20um%20dos%20princípios,ações%20e%20serviços%20de%20saúde.>. Acesso em: junho de 2023

FLORIDI, Luciano. **The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU.** Philos. Technol. 33, 369–378 (2020). Disponível em: <https://doi.org/10.1007/s13347-020-00423-6>. Acesso em: julho de 2023.

GOSWAMI, Swish. ***What Does Big Tech Actually Do With Your Data?***. Site da internet, 2022. Disponível em <https://www.forbes.com/sites/forbestechcouncil/2022/02/16/what-does-big-tech-actually-do-with-your-data/?sh=b203487515f7>. Acesso em: julho de 2023.

GROSSMANN, Luís. **Com AWS, Huawei e Google, Extreme Digital vence pregão de nuvem federal por R$ 65 milhões.** Site da internet, 2021. Disponível em <https://www.convergenciadigital.com.br/Cloud-Computing/Com-AWS%2C-Huawei-e-Google%2C-Extreme-Digital-vence-pregao-de-nuvem-federal-por-R%24-65-milhoes-56581.html?UserActiveTemplate=mobile> Acesso em: maio de 2023.

GRIFFITHS, Charles.***The Latest Cloud Computing Statistics (updated July 2023).*** Site da internet, 2023. Disponível em <https://aag-it.com/the-latest-cloud-computing-statistics/#:~:text=Headline%20Cloud%20Computing%20Statistics%20for%202023&text=In%20total%2C%20Amazon%2C%20Microsoft%20and,in%202022%20was%20%24111%20billion>. Acesso em: maio de 2023.

GUZMANM et al (2019). ***Amazon Comprehend Medical and AI in Healthcare.*** Disponível em <https://nyupau.github.io/posts/amazon_comprehend/>. Acesso em: julho de 2023.

HIMSS, Healthcare Information and Management Systems Society. ***HIMSS Defines Digital Health for the Global Healthcare Industry.*** Disponível em < https://www.himss.org/news/himss-defines-digital-health-global-healthcare-industry>. Acesso em: julho de 2023.

JUNIOR, Luiz. **Computação em Nuvem no Governo - Aspectos Organizacionais, Institucionais e Contextuais**. São Paulo: Fundação Getulio Vargas (FGV-EAESP), 2020. Disponível em <https://bibliotecadigital.fgv.br/dspace/handle/10438/29736>. Acesso em: maio de 2023.

KOIKE, Beth. **Intermédica avalia IPO e novo sócio estrangeiro**. Site da internet, 2017. Disponível em <https://valor.globo.com/empresas/noticia/2017/03/07/intermedica-avalia-ipo-e-novo-socio-estrangeiro.ghtml>. Acesso em: maio de 2023.

KWET, Michael. (2019). ***Digital colonialism: US empire and the new imperialism in the Global South.*** Race & Class, 60(4), 3–26. <https://doi.org/10.1177/0306396818823172>

LACERDA, Nara. **Dados públicos brasileiros podem parar nas mãos da iniciativa privada.** Agosto de 2020. Disponível em <https://www.brasildefato.com.br/2020/08/02/dados-publicos-brasileiros-podem-ir-parar-nas-maos-da-iniciativa-privada>. Acesso em: maio de 2023.

LAINE, Jorge. **O neocolonialismo do ouro verde**. INCI v.34 n.6 Caracas jun. 2009. Disponível em <http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S0378-18442009000600003>. Acesso em: maio de 2023.

LEMES, Marcelle; LEMOS, Amanda. **O uso da inteligência artificial na saúde pela Administração Pública Brasileira.** Cadernos ibero-americanos de direito sanitário, 2020. Disponível em <https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/684> Acesso em: julho de 2023.

LERMAN, Rachel; SHABAN, Hamza. ***Amazon will see you now: Tech giant buys health-care chain for $3.9 billion***. The Washington Post, 21 de julho de 2022. Disponível em <https://www.washingtonpost.com/business/2022/07/21/amazon-health-care/> Acesso em: julho de 2023.

LIMA, Jefferson da Costa. **Desafios para a adoção de Inteligência Artificial pelo Sistema Único de Saúde (SUS): ética, transparência e interpretabilidade**. 2022. 146 f. Tese (Doutorado em Informação e Comunicação em Saúde) - Instituto de Comunicação e Informação Científica e Tecnológica em Saúde, Fundação Oswaldo Cruz, Rio de Janeiro, 2022. . Acesso em: maio de 2023.

LIMA, Jefferson. **Desafios para a adoção de Inteligência Artificial pelo Sistema Único de Saúde (SUS): ética, transparência e interpretabilidade**. Fundação Oswaldo Cruz, Instituto de Comunicação e Informação Científica e Tecnológica em Saúde, julho de 2022. Disponível em <https://www.arca.fiocruz.br/bitstream/handle/icict/55992/jefferson_lima_icict_dout_2022.pdf?sequence=2&isAllowed=y>. Acesso em julho de 2023.

LIPPOLD, W.; FAUSTINO, D. **Colonialismo digital, racismo e acumulação primitiva de dados. Germinal: marxismo e educação em debate**, [S. l.], v. 14, n. 2, p. 56–78, 2022. Disponível em: https://periodicos.ufba.br/index.php/revistagerminal/article/view/49760. Acesso em: maio de 2023.

MACHADO, Letícia; TAVARES, Sara. **Programa TechSUS - Governança e interoperabilidade de dados para a Saúde**. Instituto de Estudos para Políticas de Saúde, 2023. Disponível em <https://static.poder360.com.br/2023/03/panorama-ieps-4-techSUS-saude-digital.pdf>. Acesso em: maio de 2023.

MARCHIORI, Brenda. **Dependência da produção internacional de medicamentos pode explicar escassez no mercado.** Site da internet, 2022. Disponível em

<https://jornal.usp.br/atualidades/falta-de-investimento-em-ciencia-e-pesquisa-agrava-escasse z-de-medicamentos-no-mercado/>. Acesso em: maio de 2023.

MARINI, R. M. **Dialética da Dependência. Germinal: marxismo e educação em debate**, [S. l.], v. 9, n. 3, p. 325–356, 2017. DOI: 10.9771/gmed.v9i3.24648. Disponível em <https://periodicos.ufba.br/index.php/revistagerminal/article/view/24648> Acesso em: 27 jul. 2023. . Acesso em: maio de 2023.

MARINHO, Márcia. **Revisão da Política Nacional de Informação Informática (PNIIS).** Fórum da RNDS, 2020. Disponível em <https://www.gov.br/saude/pt-br/composicao/seidigi/saude-digital/material-de-apoio/CBIS2020_RevisaodaPoliticaNacionaldeInformacaoeInformatica.pdf> . Acesso em: maio de 2023.

MARGI, Cítia. **Hackers acessaram nuvem do Ministério da Saúde com senha; entenda o ataque.** USP, Escola Politécnica, 2021. Disponível em <https://www.poli.usp.br/noticias/polinamidia/63258-hackers-acessaram-nuvem-do-ministerio-da-saude-com-senha-entenda-o-ataque.html>. Acesso em: maio de 2023.

MARRANO, Beatriz. **O que é Colonialismo?** UNIPAMPA, Laboratório de Estudos em História do Mundo Árabe e Islã, agosto de 2021. Disponível em <https://sites.unipampa.edu.br/lehmai/o-que-e-colonialismo/> Acesso em maio de 2023.

MARTINS LEMES, M.; NUNES LOPES ESPIÑEIRA LEMOS, A. **O uso da inteligência artificial na saúde pela Administração Pública brasileira.** Cadernos Ibero-Americanos de Direito Sanitário, [S. l.], v. 9, n. 3, p. 166–182, 2020. DOI: 10.17566/ciads.v9i3.684. Disponível em <https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/684> Acesso em julho de 2023.

MORAES, Ilara. **Prontuário Eletrônico Único e a Transformação Digital na Saúde.** Câmara dos Deputados Comissão de Seguridade Social e Família Audiência Pública, 13 de dezembro de 2022. Acesso em julho de 2023.

MOTORYN, Paulo. **Diretor que levou dados do SUS para Amazon deixou gestão Bolsonaro para trabalhar na empresa.** Site da internet, 2022. Disponível em <https://www.brasildefato.com.br/2022/03/24/diretor-que-levou-dados-do-sus-para-amazon-deixou-gestao-bolsonaro-para-trabalhar-na-empresa> . Acesso em: maio de 2023.

NAVARRETE, Ana. **Desregulamentação da Saúde suplementar**. 2017. Disponível em <https://www.dgabc.com.br/Noticia/2628157/desregulamentacao-da-saude-suplementar> . Acesso em: maio de 2023.

NAVARRETE, Helena. **O plano CEIBAL e a construção de ambientes de comunicação**. 2014. Disponível em <https://static.casperlibero.edu.br/uploads/2014/04/Helena-Maria-Cecilia-Navarrete.pdf> . Acesso em: maio de 2023.

NEVES, Gabriela. **Governança da Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD 28) e o Programa Conecte SUS.** Brasília, 08 de novembro de 2022. Disponível em <https://cosemsgo.org.br/wp-content/uploads/2022/11/Governanca-da-ESD28-e-Programa-Conecte-SUS.pdf> Acesso em julho de 2023.

NETO, Amorim. **A crise política brasileira de 2015-2016: Diagnóstico, sequelas e profilaxia**. 2016. 43-54. Disponível em <https://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri52/RI52_art04_OAN.pdf>. Acesso em julho de 2023.

NIC.BR; CETIC.BR. **A transformação digital nos sistemas de saúde.** Panorama Setorial da Internet n° 1, 2022. Disponível em <https://cetic.br/pt/publicacoes/indice/panoramas/> Acesso em maio de 2023.

NIC.BR; CETIC.BR. **TIC Governo eletrônico: Pesquisa sobre o uso das tecnologias de informação e comunicação no setor público brasileiro**. São Paulo: Comitê Gestor da Internet no Brasil, 2021. Disponível em <https://cetic.br/media/docs/publicacoes/2/20220725170710/tic_governo_eletronico_2021_livro_eletronico.pdf> Acesso em maio de 2023.

NIC.BR; CETIC.BR. **Proteção de dados pessoais: privacidade e confiança no ambiente digital.** Panorama Setorial da Internet, Número 2, Junho de 2023, Ano 15. Disponível em <https://cetic.br/media/docs/publicacoes/6/20230727104116/psi-ano-xv-n-2-protecao-de-dados-pessoais.pdf> Acesso em maio de 2023.

NIST, National Institute of Standards and Technology. ***The NIST Definition of Cloud Computing.*** Estados Unidos, setembro de 2011. **Disponível em <**https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf>

OBERMEYER et al (2019). **Dissecting racial bias in an algorithm used to manage the health of populations.** Science 366, 447–453. Disponível em <doi: 10.1126/science.aax2342.>. Acesso: junho de 2023.

OLIVEIRA, Thaís. **Aspectos Gerais para adequação da RNDS à LGPD**. Brasília, 08 de novembro de 2022. Disponível em <https://cosemsgo.org.br/wp-content/uploads/2022/11/Aspectos-Gerais-para-adequacao-da-RNDS-a-LGPD.pdf> . Acesso em: maio de 2023.

OZALP et al. (2022). "***Digital Colonization" of Highly Regulated Industries: An Analysis of Big Tech Platforms' Entry into Health Care and Education***. California Management Review, 64(4), 78–107. . Acesso em: maio de 2023.

PASSOS, Juliana. **A falta de integração e distribuição das bases de dados fragiliza sistemas de informação em saúde no país**. Site da internet, 2022. Disponível em <https://www.epsjv.fiocruz.br/noticias/reportagem/falta-de-integracao-e-distribuicao-das-bases-de-dados-fragiliza-sistemas-de> . Acesso em: maio de 2023.

PICKERT, Lorena. **Big Techs: o que são e o que esperar das gigantes da tecnologia em 2023?**. Novembro de 2022. Disponível em <https://blog.aaainovacao.com.br/bigh-techs-gigantes-da-tecnologia/#:~:text=As%20Big%20Five%20(Apple%2C%20Amazon%2C%20Alphabet%2C%20Microsoft%20e,de%20quatro%20nações%20do%20G20.>. Acesso em: maio de 2023.

PINTO, Renata. **Soberania digital ou colonialismo digital?: novas tensões relativas à privacidade, segurança e políticas nacionais**. Revista Internacional de Direitos Humanos, São Paulo, v. 15, n. 27, p. 15-28, jul. 2018. Disponível em: <https://bdjur.stj.jus.br/jspui/handle/2011/127003>. Acesso em: maio de 2023.

PONEMON INSTITUTE. ***Cyber Insecurity in Healthcare:The Cost and Impact on Patient Safety And Care.*** 2022. Disponível em <https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-cyber-insecurity-healthcare-ponemon-report.pdf>. Acesso em: março de 2023

PRINGLE, Eleanor. ***Andy Jassy has identified Amazon's next frontiers—and they have nothing to do with selling books or gadgets***. Site da internet, 2023. Disponível em <https://fortune.com/2023/04/13/amazon-ceo-andy-jassy-shareholders-focus-on-health-care-grocery-office-supply-markets/>. Acesso em: maio de 2023.

QUEIROZ, Luiz. **CGU derruba parte do sigilo imposto pelo Serpro para não revelar "parceria" com a AWS**, 2023. Disponível em <https://capitaldigital.com.br/cgu-derruba-parte-do-sigilo-imposto-pelo-serpro-para-nao-revelar-parceria-com-a-aws/> Acesso em: março de 2023.

RACHID, Raquel Requena; FORNAZIN, Marcelo; COELHO NETO, Giliate Cardoso. **A saúde digital nos últimos quatro anos e os desafios para o novo governo. 2022.** Revista Eletrônica de Comunicação, Informação & Inovação em Saúde, Rio de Janeiro, v. 16, n. 4, p. 753-758. 2023. DOI: 10.29397/reciis.v16i4.3515. Acesso em: maio de 2023.

RACHID, Raquel; FORNAZIN, Marcelo; CASTRO, Leonardo; GONÇALVES, Luis Henrique; PENTEADO, Bruno. **Saúde digital e a plataformização do Estado brasileiro**. Cien Saude Colet [periódico na internet] (2023/Jan). Disponível em <https://cienciaesaudecoletiva.com.br/artigos/saude-digital-e-a-plataformizacao-do-estado-brasileiro/18635?id=18635> Acesso em: maio de 2023.

ROSALES, Luana. **Ministério da Saúde migra para AWS com Embratel.** Site da internet, 2020. Disponível em <https://www.baguete.com.br/noticias/22/04/2020/ministerio-da-saude-migra-para-aws-com-embratel> Acesso em: junho de 2023.

SAMMARCO, Ana. **Ministério da Saúde atualiza Política de Informação e Informática**. Site da internet, 2021. Disponível em <https://www.mattosfilho.com.br/unico/ministerio-saude-politica-informacao-informatica-saude/> Acesso em: julho de 2023.

SANTAELLA, L., & KAUFMAN , D. (2021). **Os dados estão nos engolindo?**. Civitas: Revista De Ciências Sociais, 21(2), 214–223. <https://doi.org/10.15448/1984-7289.2021.2.39640>. Acesso em: junho de 2023.

SANTOS, Rahellen. **O que é o Marco Civil da Internet?.** Agosto de 2021 Disponível em <https://www.politize.com.br/marco-civil-da-internet/>. Acesso em: junho de 2023.

SANTOS, Cleberson. **Marco Civil da Internet: Cinco anos depois, o que mudou?.** Março de 2019. Disponível em <https://www.nic.br/noticia/na-midia/marco-civil-da-internet-cinco-anos-depois-o-que-mudou/>. Acesso em: junho de 2023.

SCHEFFER, Mário; SOUZA, Paulo. **A entrada do capital estrangeiro no sistema de saúde no Brasil.** Cadernos De Saúde Pública n°38, 2022. Disponível em <https://doi.org/10.1590/0102-311X00239421>. Acesso em maio de 2023.

SETIC, Secretaria de Tecnologia da Informação e Comunicação. **Termo de Referência - Infraestrutura de nuvem. 2022**. Disponível em <https://www.csjt.jus.br/documents/955023/0/2022___TR___v7___Adesao_a_ARP_n__11_2021___Nuvem_JT_assinado.pdf/93ce7401-c178-f678-e1e8-a6dc8ded3bd8?t=1664545892493 > Acesso em maio de 2023.

SILVA, Vinícius. **Uso de Nuvem pelo Setor Público BrasileiroOportunidades e Desafios, Modelo NuvemGov e Gestão de Riscos de Aplicações em Nuvem**. Brasília, 2018. Disponível em <http://www.integrati.ufpr.br/portal/integrati2017/wp-content/uploads/sites/5/2018/04/Uso-de-Nuvem-pelo-Setor-Público-Brasileiro-UFPR.pdf> Acesso em maio de 2023.

SIQUEIRA, Alessandra. (2021). **O colonialismo digital como nova forma de imperialismo na sociedade em rede**. DIKÉ – Revista Do Programa De Pós-Graduação em Direito Da Universidade Federal De Sergipe, 8(1), 29-50. Disponível em <https://www.seer.ufs.br/index.php/dike/article/view/15223>. Acesso em: junho de 2023.

SOLVER. ***Your personal data may be Big Tech's most profitable product. It also may be one you would be willing to pay them to stop selling.*** Site da internet, 2021. Disponível em <https://groupsolver.com/blog/groupsolver-insights/your-data-is-big-techs-most-profitable-product/> Acesso em: junho de 2023.

SOUZA, Delton. **Discriminação algorítmica nas plataformas de e-commerce: análise crítica das principais práticas.** UNIFG, 2022. Disponível em <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/28483/1/TCC%20II%20%283%29.pdf> Acesso em: maior de 2023.

SOUZA, Joyce. I**nteligência artificial, algoritmos preditivos e o avanço do colonialismo de dados na saúde pública brasileira.** In: AMADEU, S., SOUZA, J., CASSINO, J. **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal.** Brasil: Autonomia Literária, 2021. p.(109-127). Acesso em: maio de 2023.

STATISTA. ***Big Three Dominate the Global Cloud Market.*** Abril de 2023. Disponível em <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers/#:~:text=According%20to%20estimates%20from%20Synergy,33%20percent%20in%20Q4%202022.>. Acesso em: junho de 2023.

STATISTA. ***Cloud infrastructure services vendor market share worldwide from 4th quarter 2017 to 4th quarter 2022.*** 27 de fevereiro de 2023. Disponível em <https://www.statista.com/statistics/967365/worldwide-cloud-infrastructure-services-market-share-vendor/>. Acesso em: junho de 2023.

STATISTA. ***Global market share held by operating systems for desktop PCs, from January 2013 to January 2023.*** Fevereiro de 2023. Disponível em <https://www.statista.com/statistics/218089/global-market-share-of-windows-7/#:~:text=Microsoft%20Windows%20was%20the%20dominant,of%20just%20over%2074%20percent.>

STATISTA**.** ***Global net revenue of Amazon from 2014 to 2022, by product group***. Fevereiro de 2023. Disponível em <https://www.statista.com/statistics/672747/amazons-consolidated-net-revenue-by-segment/> Acesso em: junho de 2023.

STATISTA. ***Market share of leading desktop search engines worldwide from January 2015 to March 2023.*** Maio de 2023. Disponível em <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>. Acesso em: junho de 2023.

TECNOPOLÍTICA #62: **Não se assuste: os termos de uso das plataformas que atuam na Educação.** Entrevistadas: Stephane Lima; Marina Meira. Entrevistador: Sergio Amadeu da Silveira. [S. l.]: set. 2020. Podcast. Disponível em: https://open.spotify.com/episode/3SYVDGyIjbFucNzCOVCbDq . Acesso em: junho de 2023.

THE ECONOMIST. **The world's most valuable resource is no longer oil, but data.** Maio de 2017. **Disponível em <**https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data> Acesso em: junho de 2023.

TONIAL, Felipe Augusto Leques; MAHEIRIE, Kátia; GARCIA JR, Carlos Alberto Severo. **A resistência à colonialidade: definições e fronteiras**. Rev. Psicol. UNESP, Assis , v. 16, n. 1, p. 18-26, jun. 2017 . Disponível em <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1984-90442017000100002&lng=pt&nrm=iso>. Acesso em: junho de 2023.

WEST, Emily. ***Amazon: Surveillance as a Service.*** .Surveillance & Society, 17. (27-33), 2019. DOI: 10.24908/ss.v17i1/2.13008. Acesso em: junho de 2023.

WORLD HEALTH ORGANIZATION (WHO). **Global strategy on digital health 2020-2025**. Genebra: A Organização, 2020. Disponível em: <https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pd>. Acesso em: junho de 2023.

ZUBOFF, Shoshana. **Um capitalismo de vigilância.** Site da internet, 3 de janeiro de 2019. Disponível em <https://diplomatique.org.br/um-capitalismo-de-vigilancia/>. Acesso em: junho de 2023.