Cadernos NAUI
Núcleo de Dinâmicas Urbanas e Patrimônio Cultural

Dossiê: Colonialismo digital, fluxos de informação e autoria em tempos de inteligência artificial

v 14 | n 27 | jul-dez 2025

Saúde e proteção de dados pessoais: direitos conflitantes?

Júlia Guilherme Delmondes; Érica Quinaglia Silva

Edição eletrônica
URL: NAUI – Dinâmicas Urbanas e Patrimônio Cultural (ufsc.br)

ISSN: 2558 - 2448

Organização
Núcleo de Dinâmicas Urbanas e Patrimônio Cultural

Programa de Pós-Graduação em Antropologia Social da UFSC

Referência Bibliográfica

DELMONDES, Júlia Guilherme; SILVA, Érica Quinaglia. Saúde e proteção de dados pessoais: direitos conflitantes?. Cadernos Naui: Núcleo de Dinâmicas Urbanas e Patrimônio Cultural, Florianópolis, v. 14, n. 27, p. 147-175, jul-dez 2025. Semestral.

Saúde e proteção de dados pessoais: direitos conflitantes?

Júlia Guilherme Delmondes[1]

Érica Quinaglia Silva[2]

Resumo

Esta etnografia de/em documentos teve como objetivo verificar um possível conflito entre a saúde e a proteção de dados pessoais, direitos fundamentais constitucionalmente previstos, em um contexto em que novas formas de biopoder são exercidas pelo capitalismo de vigilância, com técnicas que permitem a rastreabilidade da vida e a monetização de dados pessoais. A fim de compreender a atuação do Estado e do mercado por meio de normas, políticas, disputas e silenciamentos no contexto pandêmico, buscou-se mostrar as falhas na proteção de dados em saúde. O uso de dados, quando devidamente regulamentado, pode contribuir para um fluxo informacional seguro e íntegro, inclusive em meios acadêmicos, a exemplo de pesquisas em saúde, e colaborar para a implementação de políticas públicas em saúde e a consequente materialização do direito à saúde. Por outro lado, os interesses governamentais e as ambições corporativas por vezes são sobrepostos aos direitos humanos e às garantias fundamentais. Se não são direitos conflitantes, saúde e proteção de dados pessoais podem assim se colocar diante de uma gestão em saúde mediada pela hiperconectividade sem a devida regulamentação e atenção a especificidades no que diz respeito ao tratamento de dados em saúde.

Palavras-chave: direito à saúde; direito à proteção de dados pessoais; biopoder; Estado.

Health and personal data protection: conflicting rights?

Abstract

This ethnography of/in documents aimed to verify a possible conflict between health and personal data protection, fundamental rights constitutionally provided, in a context in which

[1] Bacharela em Saúde Coletiva pela Universidade de Brasília. Link para o Currículo Lattes: http://lattes.cnpq.br/1498435731059993. ORCID: https://orcid.org/0009-0002-1304-3117. E-mail: ju.delmondess@gmail.com.

[2] Antropóloga e professora na Universidade de Brasília. Bolsista de Produtividade em Pesquisa do Conselho Nacional de Desenvolvimento Científico e Tecnológico. Link para o Currículo Lattes: http://lattes.cnpq.br/7125713612136155. ORCID: https://orcid.org/0000-0001-9526-7522. E-mail: equinaglia@yahoo.com.br.

new forms of biopower are exercised by surveillance capitalism, with techniques that allow the traceability of life and the monetization of personal data. In order to understand the actions of the State and the market through norms, policies, disputes and silences in the pandemic context, we sought to show the flaws in the protection of health data. The use of data, when properly regulated, can contribute to a safe and complete flow of information, including in academic circles, such as health research, and collaborate in the implementation of public health policies and the consequent materialization of the right to health. On the other hand, government interests and corporate ambitions sometimes take precedence over human rights and fundamental guarantees. If they are not initially conflicting rights, health and personal data protection may become so in the face of health management mediated by hyperconnectivity without due regulation and attention to specificities regarding the processing of health data.

Keywords: right to health; right to personal data protection; biopower; State.

Salud y protección de datos personales: ¿derechos en conflicto?

Resumen

Esta etnografía de/en documentos tuvo como objetivo verificar un posible conflicto entre la salud y la protección de datos personales, derechos fundamentales previstos constitucionalmente, en un contexto en el que nuevas formas de biopoder son ejercidas por el capitalismo de vigilancia, con técnicas que permiten la trazabilidad de la vida y la monetización de datos personales. Con el objetivo de comprender la actuación del Estado y del mercado a través de normas, políticas, disputas y silencios en el contexto de la pandemia, buscamos mostrar las fallas en la protección de datos de salud. El uso de datos, cuando está adecuadamente regulado, puede contribuir a un flujo seguro y completo de información, incluso en entornos académicos, como la investigación en salud, y colaborar en la implementación de políticas de salud pública y la consecuente materialización del derecho a la salud. Por otra parte, los intereses gubernamentales y las ambiciones corporativas a veces prevalecen sobre los derechos humanos y las garantías fundamentales. Si bien inicialmente no son derechos conflictivos, la salud y la protección de datos personales pueden llegar a serlo ante una gestión sanitaria mediada por la hiperconectividad sin la debida regulación y atención a las especificidades respecto del tratamiento de datos de salud.

Palabras clave: derecho a la salud; derecho a la protección de datos personales; biopoder; Estado.

Introdução

A tecnologia é um significativo artifício que contribui para a resistência e as adaptações de indivíduos à sociedade. Desde a pré-história até a contemporaneidade, é indubitável que a tecnologia seja inerente à vida humana: gera e é gerada pelo conhecimento humano em prol de sua (sobre)vivência nas relações ambientais e socioculturais. Seja ela entendida como material, a exemplo de máquinas, equipamentos, aparelhos, ferramentas ou instrumentos, seja ela compreendida como técnica, habilidades, procedimentos e modos de fazer que sujeitos desenvolvem no seu cotidiano, o que é possível afirmar é que a tecnologia é um processo associado ao conhecimento humano tencionado à geração e utilização de produtos com o propósito de organizar as relações humanas (Lorenzetti *et al.*, 2012).

Podem ser considerados os primeiros instrumentos tecnológicos da história da humanidade os artefatos advindos da pedra lascada com o propósito de sobrevivência do hominídeo, contribuindo para as práticas de caça e defesa e para a organização da comunidade. Nesse sentido, a tecnologia caracteriza-se pelo conjunto de saberes necessários para a idealização e para a criação de artefatos, sistemas, processos e ambientes desenvolvidos pelo ser humano com o propósito de satisfazer necessidades e pretensões pessoais e coletivas (Veraszto *et al.*, 2009).

Ainda no período paleolítico, o homem dominou o fogo com base na técnica de friccionar pedras ou madeiras, e o domínio técnico sobre esse elemento natural na primeira fase da pré-história impactou significativamente o cotidiano dos hominídeos e acarretou o desenvolvimento de novas tecnologias que favoreceram a evolução humana. Esse foi um triunfo sobre as adversidades existentes e um grande aliado para o desenvolvimento tecnológico na história da humanidade.

O domínio do fogo marcou também o período histórico conhecido como Revolução Industrial, no qual máquinas eram movidas a vapor proveniente da queima de carvão, sendo esse período responsável por estabelecer importantes transformações econômicas, tecnológicas e sociais, bem como a substituição da manufatura pela maquinofatura, cenário no qual o trabalho humano foi comutado pelo trabalho de máquinas capacitadas para realizarem funções com maior precisão e de forma mais rápida (Rocha *et al.*, 2020).

Em meados do século XIX, o carvão, o vapor e o ferro foram substituídos pela eletricidade, pela química e pelo petróleo, caracterizando o princípio da Segunda Revolução Industrial. De acordo com Rocha, Lima e Waldman (2020), esse período foi marcado por

avanços tecnológicos, pelo fortalecimento do sistema econômico capitalista e por avanços nos âmbitos das telecomunicações, dos transportes e da saúde, bem como pelo desenvolvimento da política de expansão externa, o imperialismo, que alcançou, sobretudo, a Ásia, a África e a América Latina.

A Terceira Revolução Industrial iniciou-se a partir da segunda metade do século XX, quando a informação se tornou a matéria-prima mais importante pela chegada da informática, da internet, dos computadores pessoais e de outras tecnologias da informação e comunicação que revolucionaram os âmbitos do trabalho, da comunicação e do campo científico, com destaque para as áreas da robótica e da genética. Essa era contribuiu também para a industrialização dos países e para o fenômeno da globalização por meio de uma integração econômica e política baseada no avanço tecnológico dos sistemas de comunicação e de transporte (Rocha *et al.*, 2020).

De acordo com Schwab (2016) e Rocha *et al.* (2020), experienciamos uma Quarta Revolução Industrial, conhecida também como Indústria 4.0, que se caracteriza pela mudança na forma que vivemos, tanto laboral como relacional, tendendo a ser automatizada a partir das tecnologias da informação e comunicação desenvolvidas no período anterior e aperfeiçoadas na era atual, sendo essa automação baseada em sistemas que associam as máquinas com processos digitais, a exemplo da Internet das Coisas (IoT), que se refere a uma rede de dispositivos físicos equipados com sensores, softwares e outras tecnologias, permitindo a conexão e o intercâmbio de dados com outros aparelhos e sistemas por meio da internet. Esses dispositivos podem ser desde itens domésticos simples até equipamentos industriais avançados (Oracle Corporation, 2025), como lâmpadas que acendem por comando de voz e geladeiras que monitoram alimentos e fazem listas de compras.

Um dos alicerces da atual revolução industrial é o *big data*, que são os dados coletados, armazenados e tratados que influenciam o trabalho conjunto dessas máquinas e sistemas em nossa sociedade informacional e tecnológica. Posto isso, pode-se afirmar que o uso das tecnologias da informação e comunicação e o uso de dados pessoais são substanciais para que o sistema econômico atual exerça sua funcionalidade em nossa sociedade organizacional hiperconectada e vigiada.

No âmbito da saúde, a tecnologia aplicada fomenta inúmeros avanços e soluções. Os benefícios são testemunhados na prestação e gestão de serviços em saúde, nos modernos equipamentos utilizados que cada dia progridem ainda mais, enquanto a educação, comunicação e informação são fortemente impactadas pelos avanços tecnocientíficos. Na Era

Técnico-Científico-Informacional, como também é conhecido o período que experienciamos, as informações e seus segmentos, os dados, transitam com grande intensidade e velocidade.

Atualmente, a gestão e análise de dados, bem como a gestão informacional são fundamentais para o planejamento, a organização, a direção e o controle de diferentes áreas da sociedade, inclusive no âmbito sanitário. Ações gerenciais e operacionais em saúde vêm sendo transformadas com a aplicação de análise de dados em conjunção com o uso das Tecnologias da Informação e Comunicação (TIC). Essas ações vêm colaborando para um modelo de atenção integral que proporciona ao indivíduo uma atenção à saúde de qualidade, uma vez que a análise de dados possibilita uma melhor interpretação das tendências em saúde dos usuários, tratamento personalizado e prevenção de doenças, contribuindo também para a tomada de decisões baseada em evidências, melhoria no atendimento e otimização da eficiência operacional (Datasigh, 2023).

As TIC em saúde configuram-se como um conjunto de ferramentas tecnológicas e computacionais que englobam recursos de hardware, software, sistemas de telecomunicações e de gestão de dados e informações, com os objetivos de mediar processos comunicacionais e auxiliar o gerenciamento em saúde. As TIC em saúde ampliam o acesso aos serviços e podem colaborar para a redução de ineficiências e custos e, assim como a análise de dados, proporcionam um atendimento individualizado, que considera as distintas expectativas e necessidades dos usuários (Universidade de São Paulo, 2015). A utilização desse conjunto de ferramentas e serviços tecnológicos que colaboram para os processos de promoção da saúde integram o que é conhecido por *e-Health* ou e-Saúde.

Segundo a Organização Pan-Americana da Saúde (OPAS), em recente estudo, o uso da *e-Health* é seguro e possui uma boa relação de custo-benefício das TIC no suporte às diferentes esferas relacionadas à saúde, como serviços, vigilância, educação e pesquisa (Marengo *et al.*, 2023). Esse uso apresenta, contudo, tensionamentos relacionados, por exemplo, à privacidade dos dados, inclusão digital e integração entre sistemas e padronização de tecnologias.

Especificamente na pandemia de covid-19, a Saúde Digital ganhou destaque, uma vez que se alegou ser uma estratégia segura e eficaz na assistência à saúde em tempos de distanciamento e isolamento social. Entretanto, no Brasil, a expansão da Saúde Digital, o uso das TIC e de dados pessoais no âmbito da saúde ocorreram em um momento de vulnerabilidade sanitária acrescida da ausência de uma legislação específica de proteção de dados.

A e-Saúde contribuiu desde ações operacionais, como teleconsultas, prontuários e prescrições eletrônicas, até ações gerenciais nos três níveis de atenção à saúde nas esferas municipal, estadual, distrital e federal. O uso de dados pessoais configurou-se, portanto, como uma das estratégias de gestão em saúde naquele momento. Por outro lado, esse fenômeno suscita desafios.

O cenário legislativo de proteção de dados pessoais no Brasil em tempos de emergência de saúde pública encontrava-se em estado de contingência, o que evidenciou, para além de uma crise sanitária, uma crise de direitos fundamentais, especificamente do direito à proteção de dados pessoais (Quinaglia Silva e Delmondes, 2022). Essa situação ensejou um debate acerca do poder de controle do Estado mediante o domínio de dados pessoais e de uma nova configuração de biopoder exercida por estratégias de vigilância que permitem a rastreabilidade da vida, pondo em questão uma discussão sobre a sobreposição de direitos, o direito à saúde e o direito à proteção de dados pessoais. Seriam esses direitos conflitantes?

A saúde é um direito fundamental que o Estado tem por dever garantir mediante políticas públicas, conforme assegura a Constituição da República Federativa do Brasil (1988), em seu artigo 196, entre outros. A proteção de dados pessoais, que também é um direito fundamental, consta da Declaração Universal dos Direitos Humanos (DUDH, 1948), da Constituição Federal, em seu artigo 5º, X, XII e LXXII (Brasil, 1988) e também da Lei nº 13.709, de 14 de agosto de 2018 (Brasil, 2018), que entrou em vigor no dia 18 de setembro de 2020, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD).

Os dados pessoais são poderosos instrumentos de gestão em saúde. Se concentrados nas mãos de grandes empresas da área da tecnologia, conhecidas como *big techs*, sob os domínios do Estado e do mercado, os dados configuram-se como recursos de vigilância e de geração de capital. As ações que envolvem o uso de tecnologias e a consequente utilização de dados pessoais devem ser bem perscrutadas, uma vez que os interesses governamentais e mercadológicos não devem se sobrepor aos direitos humanos, às garantias fundamentais e à ética, como visto durante a gestão da pandemia de covid-19 no Brasil.

Entende-se que o uso de dados pessoais, quando devidamente regulamentado e protegido, contribui para a saúde coletiva por possibilitar o desenvolvimento de pesquisas científicas e a conseguinte formulação de políticas de cunho sanitário que visam à concretização do direito à saúde para os cidadãos brasileiros. Por outro lado, quando se analisa a conjuntura de proteção de dados no Brasil, principalmente durante a pandemia de covid-19, observa-se, além da tardia vigência da LGPD, a expedição da Medida Provisória

(MP) nº 954, que foi suspensa pelo Supremo Tribunal Federal (STF) por ferir dispositivos da Constituição Federal referentes ao artigo 5º, X, XII e LXXII, bem como o episódio do maior vazamento de dados pessoais divulgado na história do Brasil. Esses foram acontecimentos que retratam consequências desastrosas decorrentes do uso inadequado de dados pessoais e da falta de segurança informacional.

Sendo assim, torna-se importante compreender como a LGPD contribui para a prática e a pesquisa em saúde no âmbito do tratamento de dados sensíveis, uma vez que os dados clínicos são elementos de gestão econômica, sendo cobiçados pelo poder político, não somente pelo Estado, mas também pelas grandes empresas da área da informática e farmácia (Schaefer, 2010). Ainda, uma comparação entre a legislação brasileira e o regulamento europeu de proteção de dados pessoais torna-se igualmente necessária, a fim de entender como se dá a aplicação da LGPD no que tange a informações sensíveis frente à lei que foi referência para sua elaboração, o Regulamento Geral de Proteção de Dados (GDPR).

Destarte, considerado esse contexto, o objetivo deste estudo foi entender a legitimidade de novas formas de biopoder que são exercidas pelo capitalismo de vigilância, com técnicas que permitem a rastreabilidade da vida e a monetização de dados pessoais, além de um possível desrespeito a um direito fundamental, a proteção de dados pessoais, sob a justificativa de proteger outro direito fundamental, a saúde.

Metodologia

A fim de compreender, nas perspectivas da Antropologia, do Direito, da Bioética e da Saúde Coletiva, a atuação do Estado por intermédio da legislação específica de proteção de dados no que tange ao tratamento de dados em saúde e ao interesse pela digitalização de informações dos cidadãos foi utilizada uma metodologia de pesquisa qualitativa. Os dados pessoais são instrumentos de poder e de comercialização. Posto isso, as relações entre poder, controle e violação de dados pessoais em prol da gestão em saúde foram pontos importantes destacados.

A metodologia aplicada fundamentou-se em uma revisão bibliográfica e uma etnografia de/em documentos (Castro e Cunha, 2005; Cunha, 2004; Fonseca e Machado, 2015), especificamente documentos do Estado e sobre o "Estado em ação", marcado por práticas de poder e saber, disputas e silenciamentos. Para Cunha (2004), fazer uma etnografia

de/em documentos significa tratar arquivos e documentos como processos sociais, e não apenas como fontes. A autora mostra que documentos são produzidos, organizados e preservados por práticas que selecionam, classificam e também suprimem, revelando relações de poder e formas de narrar pessoas e acontecimentos. Assim, o arquivo torna-se um campo etnográfico, onde se investigam tanto os conteúdos quanto as condições e os efeitos sociais de sua produção e circulação.

Essa abordagem entende que os documentos não são registros neutros. Expressam valores, práticas e relações de poder. Compreender como eles são produzidos, circulam e são utilizados em contextos institucionais e sociais revela seus efeitos simbólicos e performativos e contribui para a construção de sentidos, a (des)legitimação de discursos e o entendimento de dinâmicas sociais.

Nessa perspectiva, a multicitada LGPD, o GDPR da União Europeia, entre outros instrumentos normativos foram referências para este trabalho. Ainda, artigos científicos, notícias veiculadas na mídia, como reportagens, artigos em sites, entre outros, compuseram este estudo. A pesquisa teve como recorte temporal o contexto pandêmico, momento no qual essas referências foram acessadas.

Todos os aspectos éticos concernentes a pesquisas científicas foram observados e respeitados. Este trabalho não foi submetido a um comitê de ética em pesquisa em virtude da excepcionalidade elencada no artigo 1°, parágrafo único, II, da Resolução n° 510, de 7 de abril de 2016, que dispõe sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais (Brasil, 2016). A pesquisa envolveu dados de acesso público.

Breve histórico da proteção de dados pessoais no Brasil

O direito à proteção de dados pessoais no Brasil, hoje garantido pela Lei Geral de Proteção de Dados Pessoais (LGPD) (Brasil, 2018), estava anteriormente presente nas entrelinhas de outras normas. Em âmbito internacional, esse direito já constava da Declaração Universal dos Direitos Humanos, estabelecida pela Organização das Nações Unidas em 1948, em seu artigo 12 (DUDH, 1948). Em âmbito nacional, a Constituição Federal já garantia esse direito desde 1988 por meio de seu artigo 5º, X, XII e LXXII (Brasil, 1988).

Ademais, outras espécies normativas, como o Código de Defesa do Consumidor, a Lei de Acesso à Informação e o Marco Civil da Internet, elencam procedimentos para a garantia do direito básico de proteção de dados (Mendes, 2017).

Esse é um direito inviolável. Contudo, sua proteção no País foi tardia, se a nossa legislação específica for comparada com outras de algumas sociedades ao redor do mundo. Em 14 de agosto de 2018, a LGPD foi sancionada pelo ex-presidente da República Michel Temer. Essa lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade (Brasil, 2018).

Desde sua sanção até sua entrada em vigor, foi uma longa, fastidiosa e um tanto quanto duvidosa jornada, tendo em vista o desastroso cenário político e sanitário no qual, após muitas incertezas, no dia 18 de setembro de 2020, a *vacatio legis* da LGPD teve seu fim (Quinaglia Silva e Delmondes, 2022).

Além da tentativa de adiar a vigência da LGPD, inexistia uma autoridade independente que pudesse supervisionar o tratamento de dados. A Autoridade Nacional de Proteção de Dados (ANPD) é um órgão da administração pública federal, integrante da Presidência da República, que tem como atribuição zelar pela proteção dos dados pessoais, nos termos da legislação. Ademais, a ANPD tem o papel fundamental de elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade (Brasil, 2018). A tardia consolidação da estrutura desse órgão também gerou questionamentos sobre a real intenção do governo federal no que diz respeito à proteção de dados pessoais (Quinaglia Silva e Delmondes, 2022).

Durante a pandemia de covid-19, conjugou-se à crise sanitária uma crise informacional no Brasil. Diante dos processos de adoecimento e morte, o uso de dados pessoais pelo Estado foi uma das alternativas de gestão implementadas. Sabe-se que, além das tardias vigência da LGPD e estruturação da ANPD, foi verificada uma tentativa de uso de dados de forma indevida, uma vez que o governo federal intentou usufruir de dados não anonimizados para a realização de pesquisas e a aplicação de monitoramento inteligente, o que tangenciou a adoção de ações que poderiam ferir a privacidade dos cidadãos (Quinaglia Silva e Delmondes, 2022).

Medidas inconstitucionais referentes ao uso de dados por parte do Estado foram tomadas, como a expedição pelo então presidente da República Jair Bolsonaro da MP nº 954, que determinava o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado (STFC) e de Serviço Móvel Pessoal (SMP) com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública decorrente do

novo coronavírus (Brasil, 2020a). Essa produção estatística ocorreria mediante o compartilhamento de dados pessoais, como nomes, números de telefone e endereços de consumidores, pessoas físicas e jurídicas, pelas empresas citadas em conjunto com o IBGE (Brasil, 2020b).

Não obstante, como mencionado, em julgamento realizado no dia 7 de maio de 2020, ela foi suspensa pelo STF por ferir dispositivos da Constituição Federal referentes ao artigo 5º, X, XII e LXXII (Brasil, 2020b; Brasil, 1988). A decisão do STF de suspender a MP nº 954 atentou para os critérios de necessidade, adequação e proporcionalidade da medida, que poderia provocar vazamentos acidentais ou o uso indevido dos dados (Quinaglia Silva e Delmondes, 2022).

Outro exemplo no qual dados pessoais de milhões de brasileiros foram divulgados sem a devida proteção ocorreu sob a justificativa de dar transparência ao pagamento do auxílio emergencial pelo governo federal para cidadãos que se encontravam em situação de vulnerabilidade social. Esses dados foram publicados no Portal da Transparência do Governo Federal, violando os direitos de privacidade e intimidade desses cidadãos, que foram ainda mais vulnerabilizados com essa medida (Privacy Tech, 2020).

Assim, como um instrumento complementar à LGPD, foi editada em 28 de março de 2023 a Portaria SGD/MGI nº 852, que institui o Programa de Privacidade e Segurança da Informação (PPSI). A norma estabelece diretrizes voltadas para a gestão de documentos e informações na administração pública, tendo como um de seus focos justamente a proteção de dados pessoais (Brasil, 2023).

Alinhada à LGPD, a portaria reforça a centralidade da privacidade e da segurança da informação como fundamentos da política institucional, mas deixa de abordar de modo mais aprofundado os aspectos políticos e sociais que atravessam o tratamento de dados sensíveis no setor público. Embora contribua para consolidar práticas administrativas voltadas para a integridade e a confidencialidade dos dados, sua efetividade depende da maturidade institucional dos órgãos públicos, da disponibilidade de recursos técnicos e humanos e de certa uniformidade na adoção das diretrizes propostas. Para que sua implementação seja eficaz – no sentido de produzir mudanças reais nas práticas institucionais –, é necessário internalizar os princípios da LGPD como elementos estruturantes da cultura organizacional.

Nesse sentido, a portaria representa um avanço normativo, mas sua capacidade de assegurar o respeito aos direitos dos cidadãos permanece condicionada à transformação substancial dos valores e das rotinas que regem a gestão pública da informação.

Vazamento de dados pessoais em período de crise sanitária

O ano de 2020 foi marcado pelo início da pandemia de covid-19. Junto com a crise sanitária, uma infodemia também foi constatada. De acordo com a Organização Mundial da Saúde (OMS), uma infodemia é "um excesso de informações, algumas precisas e outras não, que tornam difícil encontrar fontes idôneas e orientações confiáveis quando se precisa" (OPAS, 2020).

Houve entre 2020 e 2022 uma grande propagação de notícias, que por vezes caracterizaram-se como falsas, sendo conhecidas como *fake news*. O próprio governo Bolsonaro divulgou essas notícias em circunstâncias de minimização da magnitude da pandemia e do incentivo à realização de um tratamento denominado precoce que não possuía qualquer fundamentação científica, ao invés de disseminar dados científicos sérios e propiciar o uso da vacina com a urgência que o cenário de calamidade requeria. Essas desinformações impactaram significativamente a saúde coletiva.

Ademais, esse cenário de desordem informacional e de insegurança sanitária foi impactado pelo maior vazamento de dados da história do Brasil. Essa catástrofe aconteceu no dia 20 de janeiro de 2021, quatro meses depois de a LGPD entrar em vigor. Essa lei não foi, portanto, suficiente para impedir que dados de 223 milhões de brasileiros, quantidade maior que a própria população brasileira, porque contava com informações de cidadãos falecidos, fossem divulgados sem a devida proteção (Belli, 2022).

Como consequência da exposição de informações, como nomes, datas de nascimentos, endereços, fotos de rostos, impostos de renda de pessoas físicas, entre outras (Portal G1, 2021), podem ser citados diversos golpes, uma vez que os cidadãos que tiveram seus dados vazados ficaram vulneráveis a fraudes, como "roubo de identidade, ou *phishing*, manipulações e discriminações por inserções em bases de dados para fins publicitários ou eleitorais desconhecidos'' (IDEC, 2021). No cenário pandêmico, destacam-se igualmente os saques de benefícios, como o auxílio emergencial e o Fundo de Garantia do Tempo de Serviço (FGTS) (Imenes, 2021; Faddul, 2021). De acordo com o Instituto Brasileiro de Defesa do Consumidor (IDEC), o megavazamento de dados configura-se como uma violação massiva ao ordenamento jurídico brasileiro de proteção de dados (IDEC, 2021).

Destarte, torna-se evidente que os dados pessoais necessitam de uma maior segurança. Mesmo diante da vigência da LGPD, os retalhos informacionais de indivíduos correm riscos perante a hiperconectividade da sociedade e dos interesses público e privado neles: uma vez divulgados, os efeitos são imediatos e perduram no longo prazo, haja vista que dados pessoais não têm data de validade; como mencionado, até mesmo dados pessoais de pessoas mortas podem ser utilizados.

O investimento em segurança de dados é uma medida imprescindível e urgente. É, portanto, necessária a atuação da ANPD, entidade fiscalizadora da lei, para combater o mercado ilegal de venda e exploração de dados.

Dados de saúde e o monopólio digitalizado

A saúde é uma das áreas nas quais a tecnologia vem ganhando mais espaço e desenvolvimento. Na pandemia de covid-19, tornou-se ainda mais evidente como as TIC contribuíram para a gestão em saúde de alguns países.

A coleta de informações de pacientes propicia, por exemplo, a identificação de doenças e o consequente tratamento. Para além da recuperação, a utilização dos dados coopera em outros níveis da atenção primária, como a própria prevenção.

O uso de dados por *startups* que atuam na área da saúde e que possuem como objetivo o desenvolvimento de inovações e soluções baseadas na aplicação de tecnologias, empresas essas conhecidas como *healthtecs*, quando devidamente regulamentado, pode contribuir para o setor saúde. Com o devido tratamento de dados sensíveis, as *healthtecs* podem colaborar para a otimização dos serviços em saúde nas esferas privada e pública. Ao analisar informações subjetivas e também coletivas, esse modelo de negócio atua desde as ações gerenciais até as operacionais.

No Brasil, o interesse em dados de saúde pode permear os eixos fundamentais da atenção à saúde, segundo os componentes das ações e dos serviços de saúde assegurados pelo Sistema Único de Saúde (SUS): promoção, proteção, prevenção, recuperação e reabilitação da saúde. Os benefícios podem se estender também para os serviços em saúde na esfera privada.

Não obstante, na sociedade da informação, os dados se caracterizam como instrumentos de monetização (Zuboff, 2021). O capitalismo de vigilância representa uma modalidade de expropriação de direitos fundamentais, como a autonomia e a liberdade, princípios centrais da Bioética e dos Direitos Humanos, que ocorre por meio da coleta

massiva de dados pessoais, seu armazenamento, seu processamento e sua subsequente comercialização, podendo comprometer a dignidade da pessoa humana e a autodeterminação informacional (Ladeia, 2020).

Nesse contexto, Joyce Souza (2021) ressalta que esse modelo de extração de dados consiste em uma tentativa sistemática de transformar todas as vidas e relações humanas em insumos para a geração de lucro, condição que ela denomina "colonialismo de dados". Tal forma de colonialização opera numa lógica em que, ao capturar e controlar a vida humana por meio da apropriação dos dados, extrai-se lucro sem que as pessoas percebam o processo em curso, reproduzindo desigualdades históricas e formas modernas de dominação.

Existe um mercado amplamente entusiasmado com o uso de dados pessoais. No sistema econômico capitalista, há um vasto comércio direcionado ao perfil e ao comportamento dos usuários, e a área da saúde não está isenta, pois hospitais, seguradoras de saúde, entre outras instituições, possuem interesse nos bancos de dados de saúde, uma vez que os benefícios advindos do domínio dessas informações são diversos. Efeitos perversos do controle desses dados são, entre outros, a vigilância contínua e invasiva, a manipulação de comportamentos, a falta de transparência e a ampliação de assimetrias de poder entre instituições e cidadãos.

Considerando, então, a primordialidade da análise sobre segurança e proteção de dados nas ferramentas e nos serviços que armazenam e utilizam informações de saúde, além dos interesses do Estado e do mercado nesses elementos, torna-se importante o debate sobre a legitimidade das novas formas de biopoder que são exercidas por meio da tecnologia, mesmo diante de uma política específica de proteção de dados pessoais no Brasil, pois os dados não são pátrios. Grande parte da infraestrutura de computação em nuvem mundial está sob o domínio de grandes empresas internacionais que dominam o mercado tecnológico, as conhecidas *big techs* (Silveira e Avelino, 2023). A computação em nuvem caracteriza-se como a oferta de serviços de computação sob demanda mediados pela internet com a funcionalidade de armazenamento, ente outros, de arquivos, redes, softwares, bancos de dados e servidores (Neto, 2019). É importante destacar que o maior investidor em pesquisas em inteligência artificial no mundo é uma das *big techs* mais renomadas e reconhecidas globalmente, a multinacional Alphabet, do grupo Google (Sociedade Brasileira de Medicina Tropical, 2023).

No Brasil, outro fato ocorrido no governo Bolsonaro que não deve ser olvidado é o da migração de dados do SUS para a nuvem Amazon Web Services (AWS). A contratação dos

serviços de uma das mais conhecidas *big techs* para o armazenamento de dados do Departamento de Informática do Sistema Único de Saúde (DATASUS) foi apoiada por Jacson Barros, ex-diretor do DATASUS, que assumiu cargo na Amazon um mês depois de se afastar da função no governo federal (Motoryn, 2022).

Informações epidemiológicas e dados de saúde estão sob o domínio da AWS. Desde 2019, o DATASUS utiliza a nuvem AWS na implementação da estratégia de Saúde Digital no Brasil, resultando na criação de variados serviços, como a Rede Nacional de Dados da Saúde (RNDS) e o Conecte SUS, plataforma utilizada por usuários do sistema público de saúde, profissionais e gestores (Amazon Web Services, 2023).

De acordo com o site de divulgação de informações sobre o SUS e o direito à saúde, Outra Saúde, embora não exista uma ilegalidade evidente nessa situação, especialistas acreditam que o caso deve ser examinado por autoridades competentes e que o evidente conflito de interesses deve ser questionado, uma vez que a assunção de cargo na Amazon pelo ex-diretor do DATASUS pode se configurar como violação aos princípios da administração pública (Scatolini, 2022).

É, portanto, fundamental o debate acerca da soberania digital em saúde no Brasil devido ao fato de o modelo de Saúde Digital direcionar-se para o caminho da mercantilização de dados: informações epidemiológicas e dados de saúde de cidadãos brasileiros estão sob o domínio de uma das maiores empresas de tecnologia do mundo.

A biopolítica exercida durante a pandemia teve como mecanismo de aplicabilidade a tecnologia, que se configura como instrumento de exercício do biopoder. Pode-se afirmar que na área da saúde a inteligência artificial e a Saúde Digital configuram-se como poderosos artifícios para o exercício do biopoder sobre a vida dos usuários, de forma individual e coletiva (Aith, 2023). Fernando Aith destaca que, na atualidade, o principal operador e organizador do biopoder deixou de ser apenas o Estado, a maior preocupação de Foucault; agora, o biopoder emerge também dos grupos econômicos, sendo esse poder compartilhado entre governo e mercado de uma forma nebulosa e conflituosa.

Essa conjunção de fatos consolida a ideia de Cassino (2021) de que nossa vida social, convertida em dados, é um recurso que pode ser extraído e utilizado pelo capital como forma de acumulação de riquezas, sendo a população mundial fonte de informações que fundamentam o capitalismo na era digital. Tendo em vista o crescente fluxo de dados na área da saúde mediados pela *e-Health* e pela inteligência artificial, é preciso perscrutar os dispositivos e serviços que armazenam e fornecem dados sensíveis como os de saúde, bem

como aprofundar reflexões sobre as grandes empresas que estão por trás do domínio dessas informações e as relações entre domínio de dados pessoais, biopoder e negócios, visto que a manipulação do comportamento e a docilização dos corpos estão sendo possíveis por meio do uso de dados pessoais e da aplicação da inteligência artificial na saúde por intermédio de grandes empresas do setor tecnológico e da saúde, que visam acima de tudo à lucratividade.

O respeito aos direitos humanos, às liberdades fundamentais, à ética e às legislações deve ser o alicerce do exercício do biopoder mediado pela tecnologia, seja ele praticado pelo Estado, seja pelo mercado. É imprescindível que a sociedade moderna e tecnológica seja conhecedora de seus direitos e liberdades, tendo em vista um sistema de vigilância no qual a vida humana é monitorada continuamente. É preciso analisar e criticar como opera o exercício do poder sobre os corpos e as vidas e como as biopolíticas são aplicadas, dado que podem se configurar como políticas de cuidado e conservação da vida ou como necropolíticas.

Assim, considerados os benefícios e também os riscos do uso de dados de saúde, por serem eles sensíveis, ele deve ser regulamentado. Doravante, no Brasil, diante da vigência da LGPD, torna-se necessária uma maior atenção a esses dados, uma vez que sequer existe um artigo dedicado exclusivamente a essa questão. Esse será um desafio premente.

LGPD, GDPR e o tratamento de dados sensíveis

A LGPD é um dispositivo legal que tem como objetivo contribuir para um fluxo informacional seguro e íntegro, no qual se busca resguardar e amparar os direitos fundamentais de liberdade, privacidade e livre formação da personalidade do indivíduo de acordo com uma série de normas e princípios de tratamento (Brasil, 2018). Sabe-se que essa lei tem como referência a legislação europeia conhecida como *General Data Protection Regulation* (GDPR), em português, Regulamento Geral de Proteção de Dados.

O GDPR, criado pelo Parlamento Europeu e pelo Conselho da União Europeia, foi aprovado no ano de 2016 e teve sua vigência iniciada no ano de 2018. Estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (União Europeia, 2016).

Uma comparação entre ambos pode ser profícua para permitir antever os desafios que a legislação brasileira ainda precisa enfrentar para garantir uma proteção de dados mais sólida. Enquanto a LGPD estabelece dez bases legais, o GDPR determina seis. Uma base

legal se configura como um respaldo que fundamenta o tratamento de dados em determinada circunstância. Sendo assim, a base legal é uma ferramenta jurídica que justifica o tratamento de dados, seja por pessoa física ou jurídica. Para a coleta, a transmissão ou o processamento de dados pessoais, é necessária uma adequação à base da legislação específica de proteção de dados, ou seja, uma operação de dados pelo controlador e/ou operador de dados deve ser amparada e justificada por uma ou mais bases legais para que o tratamento de dados seja legal.

As bases legais da LGPD estão dispostas no Capítulo II, Seção I, referente aos requisitos para o tratamento de dados pessoais, e são as seguintes: I) o consentimento do titular dos dados; II) o cumprimento de obrigação legal ou regulatória pelo controlador; III) a execução de políticas públicas previstas em leis e/ou regulamentos, bem como asseguradas em contratos, convênios ou instrumentos congêneres; IV) a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V) a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI) o exercício regular de direitos em processo judicial, administrativo ou arbitral; VII) a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII) a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX) a atenção aos interesses legítimos do controlador ou de terceiro, salvo no caso da prevalência de direitos e liberdades do titular; e X) a proteção do crédito (Brasil, 2018).

Em comparação, as bases legais em comento estão estabelecidas simultaneamente no GDPR, exceto as que tratam da realização de estudos por órgão de pesquisa, do exercício regular de direitos, da tutela da saúde e da proteção do crédito (Neves, 2021). Não obstante, mesmo que as bases legais da LGPD configurem-se em maior quantidade quando comparadas com o GDPR, este último pode ser considerado mais restritivo e detalhado do que a legislação brasileira: o regulamento europeu é mais específico em outros quesitos, principalmente no que tange ao papel do encarregado de dados (Cátedra, 2021).

De acordo com a LGPD, o encarregado de dados é a pessoa indicada pelo controlador e operador para intermediar a comunicação entre o controlador, os titulares dos dados e a ANPD. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (Brasil, 2018).

Em relação ao tratamento de dados pessoais sensíveis – como informações sobre saúde, raça ou etnia e convicção religiosa –, dados esses que podem oferecer risco e/ou dano, a LGPD permite seu uso com consentimento explícito do titular dos dados ou responsável legal, ou seja, ele deve autorizar claramente o uso dos dados para finalidades específicas. Já o GDPR, de forma mais restritiva, proíbe a coleta, a transmissão ou o processamento dos dados sensíveis, com algumas exceções bem definidas (Brasil, 2018; União Europeia, 2016).

Dentre as 10 exceções, podem-se destacar as que se referem à saúde de forma subjetiva que contribua para a promoção, proteção e prevenção da saúde do indivíduo, bem como coletiva, quando os dados são de interesse público no âmbito da saúde pública, garantindo sobretudo o sigilo profissional. Outra circunstância na qual existe uma exceção ocorre quando o tratamento é necessário para arquivos de interesse público, investigação científica ou histórica e fins estatísticos (União Europeia, 2016).

Ainda a título de comparação, diferentemente de algumas legislações voltadas para a proteção de dados pessoais, a LGPD carece de um artigo específico para tratar de dados de saúde. Para a legislação brasileira, dados de saúde são apenas mais um tipo de dado sensível, sem um tratamento diferenciado. Assim, a LGPD oferece somente a definição de dados sensíveis, englobando e limitando todos esses termos em um só e expressando um conteúdo superficial no âmbito de dados de saúde.

Já o GDPR faz distinções importantes ao caracterizar, definir e distinguir termos como "dados de saúde", "dados genéticos e biométricos", entre outros. Especialistas como Lemos e Passos (2020) afirmam que o modelo legislativo brasileiro trata os dados de saúde como qualquer dado sensível, sem especificidade alguma, e apontam que essa falta de detalhamento na LGPD pode prejudicar a proteção desses dados.

LGPD e pesquisas em saúde

Uma lacuna para a qual será importante atentar é a proteção de dados de saúde que permeiam pesquisas. Diferentemente da legislação europeia, a LGPD conta apenas com um artigo referente a pesquisas em saúde, no qual aponta que elas, mediadas por órgãos, têm a necessidade de, sempre que possível, manter a anonimização dos titulares dos dados. Esse hiato na legislação brasileira evidencia a necessidade de regulamentação para que os impactos dessas pesquisas sejam melhor mensurados.

No Brasil, as pesquisas em saúde são atualmente regidas pela Resolução n° 466/2012

do Conselho Nacional de Saúde, que estabelece diretrizes que devem ser seguidas ao se realizar todas as pesquisas que envolvam seres humanos. Essa resolução visa assegurar os direitos e deveres dos participantes de pesquisas, da comunidade científica e do Estado. O Sistema CEP/CONEP, formado pela Comissão Nacional de Ética em Pesquisa e pelos Comitês de Ética em Pesquisa, é o sistema oficial de avaliação e monitoramento dessas pesquisas (Brasil, 2012).

Dentre os aspectos éticos elencados nesse documento, destacam-se aqueles referentes ao tratamento de dados pessoais, que, se obtidos, devem ser utilizados de acordo com o consentimento dos participantes. A resolução também enfatiza a importância da confidencialidade, da privacidade, bem como da proteção da imagem e da não estigmatização dos participantes (Brasil, 2012).

A Resolução n° 466/2012 tem como fundamento documentos internacionais e nacionais que visam à proteção dos participantes de pesquisas, especificamente de seus dados, como a própria Declaração Universal dos Direitos Humanos, o Código de Nuremberg, a Declaração Internacional sobre os Dados Genéticos Humanos e a Constituição Federal (Brasil, 2012).

Sobre a disposição do uso de dados em pesquisas em saúde na LGPD, em uma leitura sintética dessa legislação, é possível analisar que seu artigo 13 é o único referente ao tratamento de dados pessoais em estudos de saúde pública. Conforme consta desse artigo, órgãos de pesquisa poderão ter acesso a bases de dados pessoais, desde que esse acesso seja feito com responsabilidade e dentro dos limites legais. Para tanto, o tratamento desses dados deve se limitar ao órgão e à finalidade da realização de pesquisas, incluídas, sempre que possível, a anonimização ou pseudonimização dos dados (Brasil, 2018).

Há um ponto na lei que tem gerado questionamentos por não estar claramente disposto: trata-se da disposição contida no artigo 4°, II, *b*, que exclui da aplicação da LGPD os dados usados para fins exclusivamente acadêmicos. A redação desse trecho levou a ANPD a realizar o estudo técnico intitulado "A LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa". O estudo teve como objetivos: i) esclarecer o que se entende por "tratamento de dados para fins exclusivamente acadêmicos" (artigo 4º, II, *b*) e por "órgão de pesquisa" (artigo 5º, XVIII); ii) identificar as bases legais da LGPD que fundamentam o tratamento de dados pessoais para fins de pesquisas; e iii) delimitar as responsabilidades dos pesquisadores no tratamento de dados por órgãos de pesquisa (Brasil, 2022).

O estudo técnico evidencia que a LGPD prevê uma hipótese de derrogação parcial da legislação que afasta sua aplicabilidade na situação de tratamento de dados para fins exclusivamente acadêmicos (Mattos Filho, 2022). No entanto, o artigo 4º, II, *b*, tem de ser interpretado de forma restrita, limitando-se às situações em que o tratamento de dados pessoais esteja estritamente vinculado ao exercício da liberdade acadêmica. Mesmo assim, outros dispositivos da LGPD (como os arts. 6º, 8º, 10, 12 e 13) ainda podem ser aplicados (Mattos Filho, 2022; Brasil, 2018).

Esse estudo também destaca que, diante de incertezas jurídicas, impactos de cunho negativo podem ser prejudiciais para o desenvolvimento de pesquisas no País. Por isso, a LGPD propôs equilibrar a proteção dos dados pessoais com a liberdade acadêmica e o livre fluxo informacional, fundamentais para o avanço do conhecimento. Sobre o tratamento realizado para fins exclusivamente acadêmicos, o estudo expõe que o artigo 4º, II, *b*, da LGPD teve como principal objetivo "proteger a liberdade acadêmica e estabelecer um regime de proteção de dados pessoais mais flexível e mais adequado à dinâmica própria das atividades acadêmicas" (Brasil, 2022).

Ademais, o estudo explica o que a LGPD entende por "órgão de pesquisa", disposto no art. 5º, XVIII: trata-se de instituições públicas ou privadas sem fins lucrativos, com sede no Brasil, que tenham a pesquisa de caráter científico, histórico, tecnológico ou estatístico como parte da sua missão institucional. Isso significa que empresas com fins lucrativos não podem ser consideradas órgãos de pesquisa e, por isso, não podem usar certas permissões da LGPD (Mattos Filho, 2022).

Ora, esse estudo responde a algumas questões pertinentes relacionadas à LGPD no âmbito do uso de dados de saúde. Não obstante, deixa outras em aberto: Será criada uma legislação específica voltada para pesquisas em saúde? A Resolução n° 466/2012 e suas resoluções complementares, que são infralegais, continuarão em vigor?

Além disso, foi sancionada, no dia 28 de maio de 2024, a Lei nº 14.874, que dispõe sobre a pesquisa com seres humanos. Essa lei, que institui o Sistema Nacional de Ética em Pesquisa com Seres Humanos (Brasil, 2024b), foi regulamentada, no dia 7 de outubro de 2025, pelo Decreto nº 12.651. Essas normas deixam ainda dúvidas se esse sistema, que será responsável pelo controle ético de pesquisas científicas, será o atualmente vigente. Ou seja, não se sabe se o Sistema CEP/CONEP, anteriormente mencionado, continuará a existir, uma vez que não há menção nesses atos normativos sobre o papel da CONEP, somente sobre os CEP, que serão subordinados à "instância nacional de ética em pesquisa" (Brasil, 2024a).

Fortemente apoiada por representantes da indústria farmacêutica e associações de pesquisa clínica, essa lei desarticula o atual sistema de regulamentação da ética em pesquisa no Brasil, ameaça a participação e o controle sociais característicos do Conselho Nacional de Saúde – ao qual está vinculada a mencionada Resolução n° 466/2012 –, elimina a obrigatoriedade de representantes dos usuários na composição dos CEP, enfraquecendo a representação de grupos vulnerabilizados, e flexibiliza as obrigações éticas de pesquisadores e patrocinadores na oferta de medicamentos e tratamentos eficazes após a realização de estudos. Trata-se de mudanças que evidenciam uma desproteção aos participantes de pesquisas e o deslocamento dos marcos éticos da ciência em favor de interesses mercadológicos (Ciello *et al.*, 2025). Pyrrho, Barcellos e Cambraia (2024) reiteram que, em decorrência da Lei nº 14.874/2024, a CONEP e sua vinculação à esfera democrática do controle social são descontinuadas, sendo substituídas por uma instância subordinada à estrutura administrativa do Ministério da Saúde, a qual, por sua vez, está mais suscetível às pressões internacionais do que ao controle social.

Diante da realidade incerta que essa lei antevê – marcada pela ameaça ao atual sistema de regulamentação da ética em pesquisa, com resoluções que podem deixar de vigorar –, outras questões ressurgem: como será a articulação entre as leis e a resolução mencionadas? Qual será a instância responsável pela ética em pesquisas, especificamente em saúde, no País? A "instância nacional de ética em pesquisa", prevista nessa nova legislação, corresponderá à já existente CONEP, à ANPD ou será criada uma nova estrutura?

Torna-se urgente esclarecer quais serão os alcances e os limites da LGPD e da ANPD frente às pesquisas científicas que envolvem seres humanos, especificamente em saúde. A desregulamentação ética pode abrir caminho para a apropriação e o uso indevidos dos dados pessoais, especialmente em contextos de vulnerabilidade. Defender um sistema robusto de regulamentação da ética em pesquisa não é apenas uma demanda normativa, mas uma salvaguarda contra a mercantilização da vida e da dignidade humana.

Considerações finais

Vivemos na era da informação. Como consequência da globalização e da hiperconectividade, a sociedade contemporânea possui um sistema que se caracteriza como capitalismo de vigilância. Esse sistema possui interesse na digitalização do corpo humano, uma vez que nossos dados pessoais podem ser transformados em recursos monetários: o

controle social existente por intermédio do uso de dados pessoais parte de um interesse tanto público como privado (Zuboff, 2021).

Sabe-se que o conjunto de dados retrata características particulares, bem como coletivas, possibilitando o exercício do poder do Estado e do mercado sobre a sociedade. Quando devidamente utilizados e respeitados, mediante um tratamento adequado e legal, os dados contribuem para um fluxo informacional seguro e íntegro, inclusive em meios acadêmicos, a exemplo de pesquisas em saúde, e colaboram para a implementação de políticas públicas e a consequente materialização do direito à saúde (Schaefer, 2010).

Ainda na área da saúde, o uso de dados pessoais tende a contribuir para a saúde coletiva, uma vez que constituem informações relevantes para o planejamento, a promoção e a proteção da saúde. O respeito ao direito fundamental à proteção de dados pessoais nas atuais práticas de governança e de formulação de políticas públicas contribui para um mecanismo de biopoder mediado pela tecnologia que pode ser aplicado a favor da democracia, da inclusão e da proteção dos cidadãos e de seus outros direitos, como o direito fundamental à saúde (Freitas, 2020).

Não obstante, diante das novas conformações de biopoder mediadas pelo uso das tecnologias da informação e comunicação e pelo conseguinte uso de dados, tornou-se notória a tenuidade dos riscos e benefícios que a utilização dessas informações pode provocar. Se, por um lado, o uso de dados pode contribuir para a eficiência dos serviços ofertados, ele também pode, por outro lado, se configurar como instrumento de captação e dominação de recursos, podendo garantir vantagens financeiras para grandes empresas.

A modulação algorítmica – entendida como a forma pela qual algoritmos influenciam, orientam ou controlam comportamentos e decisões humanas em plataformas digitais, serviços públicos e práticas sociais – atua como um mecanismo de poder especialmente impactante em contextos de vulnerabilidades, como os decorrentes das crises sanitária e informacional. Nessas situações, ela pode gerar conflitos entre direitos fundamentais, agravados por (des)governos que demonstram desinteresse pela proteção desses direitos, como ocorreu durante a pandemia de covid-19 no Brasil. Essa crise de direitos se amplia mediante a aplicação de estratégias inconstitucionais de exploração de dados pessoais e táticas institucionais de propagação do vírus e informações falsas.

Nesse sentido, a soberania digital em saúde no Brasil se faz urgente, juntamente com o pensar e o agir críticos da sociedade diante do monopólio tecnológico existente e das práticas atuais de biopoder mediadas pelo uso da tecnologia no tratamento de dados pessoais,

especificamente em saúde. Um exemplo da dependência tecnológica brasileira frente ao poder das *big techs* é a mencionada concentração de informações da saúde pública nas mãos de uma das maiores empresas de tecnologia do mundo, a Amazon.

No capitalismo de vigilância, os interesses governamentais e as ambições corporativas por vezes são sobrepostos aos direitos humanos e às garantias fundamentais em nome do capital e do poder de controle por meio da coleta massiva de dados pessoais. Logo, o fortalecimento de políticas de proteção de dados pessoais e de uso da inteligência artificial na saúde torna-se inadiável, sobretudo diante da velocidade de transformações e evoluções tecnológicas, que, como descrito por Souza (2021), não devem ser consideradas como neutras, uma vez que esses artefatos podem possuir propriedades políticas, econômicas e sociais.

Sendo assim, torna-se imprescindível ampliar as discussões já existentes de promoção de políticas públicas voltadas à regulamentação do uso de tecnologias da informação e comunicação, bem como à criação de programas seguros, tais como os sistemas de monitoramento inteligentes, as inteligências artificiais e outras tecnologias aplicadas à saúde. Essa análise deve estar articulada a uma reflexão tanto política quanto ética.

Nota-se que as medidas para impedir o tratamento inadequado de dados pessoais ainda são insuficientes. Não à toa, para citar outro exemplo mencionado, mesmo após entrar em vigor, a LGPD não foi capaz de evitar o acesso e o compartilhamento indevidos de informações quando do megavazamento de dados durante a pandemia de covid-19. Reitera-se, portanto, a importância de investimentos em segurança da informação, de modo a garantir a confidencialidade e a integridade dos dados no País.

Quanto ao tratamento de dados em pesquisas em saúde, a coexistência da LGPD com outras legislações cria uma imprecisão normativa no Brasil. Diante desse contexto desafiador, a própria ANPD elaborou um estudo técnico a fim de esclarecer dúvidas sobre a temática. Contudo, permanecem lacunas sem serem sanadas, evidenciando um cenário de sobreposição e conflitos de normas – a LGPD, que estabelece obrigações específicas para o tratamento de dados pessoais, inclusive no âmbito de pesquisas científicas, e atribui competências à ANPD; a Resolução nº 466/2012, que possui força normativa no campo da ética em pesquisa envolvendo seres humanos no Brasil; e a Lei nº 14.874/2024, que passa a legislar sobre o mesmo tema, mas com diretrizes distintas. Essas normas incidem sobre dimensões diferentes, embora interligadas, da mesma prática – a pesquisa científica com seres humanos, especificamente em saúde –, e a forma de articulação entre elas ainda não está

suficientemente definida.

Assim, torna-se igualmente necessário refletir sobre a proteção no tratamento de dados sensíveis em saúde. Se não são a princípio direitos conflitantes, saúde e proteção de dados pessoais podem assim se tornar conflitantes diante de uma gestão em saúde mediada pela hiperconectividade sem a devida regulamentação e atenção a especificidades no que tange ao tratamento de dados em saúde.

Torna-se, destarte, indispensável que o biopoder hodiernamente mediado pela tecnologia e praticado pelo Estado e pelas grandes empresas seja convertido no respeito aos direitos fundamentais para que não haja conflito de direitos, e que o controle estatal e o capitalismo de vigilância não se sobreponham ao respeito pela dignidade da pessoa humana, além de outros princípios e direitos, como foi visto durante a pandemia de covid-19, cenário no qual se destacaram vulnerabilidades sociais, políticas e sanitárias.

Referências

AITH, Fernando. Saúde digital e IA serão instrumentos poderosos a serviço do biopoder e biopolítica. *JOTA*, 2023. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/coluna-fernando-aith/saude-digital-e-ia-serao-instrumentos-poderosos-a-servico-do-biopoder-e-biopolitica-17112023. Acesso em: 29 fev. 2024.

AMAZON WEB SERVICES. AWS suporta Datasus na implantação da Rede Nacional de Dados em Saúde (RNDS). *Amazon Web Services*, 2023. Disponível em: https://aws.amazon.com/pt/solutions/case-studies/datasus-case-study/. Acesso em: 10 dez. 2023.

BELLI, Luca. O maior vazamento de dados pessoais na história brasileira e quais lições devemos aprender. *Portal FGV*, 2022. Disponível em: https://portal.fgv.br/artigos/maior-vazamento-dados-pessoais-historia-brasileira-e-quais-licoes-devemos-aprender. Acesso em: 26 fev. 2025.

BRASIL. Autoridade Nacional de Proteção de Dados. Estudo técnico: a LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgão de pesquisa, abril de 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000810_2022_17.pdf. Acesso em: 20 jul. 2022.

BRASIL. Comissão Nacional de Ética em Pesquisa (Conep). Conep publica informe sobre alterações no sistema CEP-CONEP com a entrada em vigor da Lei nº 14.874/2024. *Centro de Pesquisa da UFF*, 2 set. 2024a. Disponível em: http://cep.uff.br/2024/09/02/conep-publica-informe-sobre-alteracoes-no-sistema-cep-conep-com-a-entrada-em-vigor-da-lei-n-o-14-874-2024/. Acesso em: 26 mar. 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. *Diário Oficial da União*, 5 out. 1988.

BRASIL. Decreto nº 12.651, de 7 de outubro de 2025. *Diário Oficial da União*, 7 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD). *Diário Oficial da União*, 14 ago. 2018.

BRASIL. Lei nº 14.874, de 28 de maio de 2024b. Dispõe sobre a pesquisa com seres humanos e institui o Sistema Nacional de Ética em Pesquisa com Seres Humanos. *Diário Oficial da União*, 28 mai. 2024.

BRASIL. Medida Provisória nº 954, de 2020a. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619. Acesso em: 20 abr. 2020.

BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. Resolução nº 466, de 12 de dezembro de 2012. *Diário Oficial da União*, 12 dez. 2012.

BRASIL. Ministério da Saúde. Conselho Nacional de Saúde. Resolução nº 510, de 7 de abril de 2016. *Diário Oficial da União*, 7 abr. 2016.

BRASIL. Notícias STF. Ministra suspende MP que prevê compartilhamento de dados com o IBGE por empresas de telecomunicações durante pandemia. *STF*, 24 abr. 2020b. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442090. Acesso em: 13 maio 2020.

BRASIL. Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre a gestão de documentos e informações no âmbito da administração pública. *Diário Oficial da União*, Brasília, DF, 28 mar. 2023. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 7 mar. 2025.

CÁTEDRA. Instituto de Desenvolvimento Profissional e Pós-Graduação. GDPR: o que é e qual a diferença em relação à LGPD. 18 ago. 2021. Disponível em: https://idcatedra.com.br/2021/08/gdpr-o-que-e-e-qual-a-diferenca-em-relacao-a-lgpd/. Acesso em: 24 maio 2022.

CASTRO, Celso; CUNHA, Olívia Maria Gomes da. Antropologia e Arquivos. *Revista Estudos Históricos*, 2(36), 2005. Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/reh/issue/view/303. Acesso em: 13 jun. 2020.

CASSINO, João Francisco. O sul global e os desafios pós-coloniais na era digital. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu (Orgs.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021. cap. 1, p. 13-31.

CIELLO, Fernando José; HARAYAMA, Rui Massato; QUINAGLIA SILVA, Érica; MALUF, Sônia Weidner. Impactos da Lei nº 14.874/2024 sobre as pesquisas nas Ciências Humanas e Sociais. Revista Ética na Pesquisa em Ciências Humanas e Sociais, v. 1, n. 1, p. 35-52, 2025.

CUNHA, Olívia Maria Gomes da. Tempo imperfeito: uma etnografia do arquivo. Mana, v. 10, p. 287-322, 2004.

DATASIGH. O papel da análise de dados na gestão de instituições de saúde. 2023. Disponível em: https://datasigh.com.br/o-papel-da-analise-de-dados-na-gestao-de-instituicoes-de-saude/#:~:text=A%20análise%20de%20dados%20desempenha%20um%20papel%20vital%20na%20gestão,operacional%20e%20prevenção%20de%20doenças. Acesso em: 21 fev. 2024.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Adotada e proclamada pela Assembleia Geral das Nações Unidas (Resolução 217 A III) em 10 de dezembro de 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 13 set. 2022.

FADDUL, Juliana. Vazamento de dados facilita golpes como saque do FGTS; saiba como se prevenir. *CNN Brasil*, 29 jan. 2021. Disponível em:

https://www.cnnbrasil.com.br/business/vazamento-de-dados-facilita-golpes-como-saque-do-fgts-saiba-como-se-prevenir/. Acesso em: 29 jul. 2022.

FONSECA, Claudia; MACHADO, Helena (Orgs.). *Ciência, identificação e tecnologias de governo.* Porto Alegre: Editora da UFRGS/CEGOV, 2015. Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/47919/Ci%2Bncia%2C%20identifica%2B%2Buo%20e%20tecnologias%20de%20governo.pdf?sequence=1&isAllowed=y. Acesso em: 13 jun. 2020.

FREITAS, Christiana. Governança tecnopolítica, biopoder e democracia em tempos de pandemia. 2020. Disponível em: https://christianafreitas.com/2020/08/governanca-tecnopolitica-biopoder-e-democracia-em-tempos-de-pandemia/. Acesso em: 5 ago. 2024.

IMENES, Martha. Crescem as tentativas de golpe com dados de pessoas mortas; veja como se proteger de cibercriminosos. *Extra*, 8 ago. 2021. Disponível em: https://extra.globo.com/economia-e-financas/crescem-as-tentativas-de-golpe-com-dados-de-pessoas-mortas-veja-como-se-proteger-de-cibercriminosos-25143241.html. Acesso em: 29 jul. 2022.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. Carta Idec no 24/2021/Coex. Gravíssimo vazamento de dados pessoais de mais de 220 milhões de brasileiros. IDEC, 2021. Disponível em: https://idec.org.br/sites/default/files/vazamento_de_dados_200_milhoes.pdf. Acesso em: 27 fev. 2025.

LADEIA, Akádja. A importância da LGPD na Bioética. Jusbrasil, 29 out. 2020. Disponível em: https://www.jusbrasil.com.br/artigos/a-importancia-da-lgpd-na-bioetica/1129183693. Acesso em: 10 abr. 2025.

LEMOS, Amanda Nunes Lopes Espiñeira; PASSOS, Edilenice. Proteção de dados pessoais em saúde: análise das legislações Brasileira e Argentina. In: ALVES, Sandra Mara Campos (Org.). *Direito sanitário: coletânea em homenagem à profa. Dra. Maria Célia Delduque.* São Paulo: Matrioska, 2020, p. 173-193.

LORENZETTI, Jorge *et al.* Tecnologia, inovação tecnológica e saúde: uma reflexão necessária. *Texto & Contexto-Enfermagem*, v. 21, p. 432-439, 2012.

MARENGO, Lívia Luize *et al.* Tecnologias móveis em saúde: reflexões sobre desenvolvimento, aplicações, legislação e ética. *Revista Panamericana de Salud Pública*, v. 46, p. e37, 2023. Disponível em: https://iris.paho.org/bitstream/handle/10665.2/56003/v46e372022.pdf?sequence=1&isAllowed=y. Acesso em: 23 nov. 2023.

MATTOS FILHO. ANPD publica estudo sobre tratamento de dados pessoais envolvendo órgãos de pesquisa. 16 de maio de 2022. Disponível em: https://www.mattosfilho.com.br/unico/anpd-orgaos-pesquisa/. Acesso em: 14 de junho de 2022.

MENDES, Laura Schertel. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. *Revista de Direito do Consumidor*, v. 106. 30 jan. 2017. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RDCons_n.106.02.PDF. Acesso em: 20 de abril de 2022.

MOTORYN, Paulo. Diretor que levou dados do SUS para Amazon deixou gestão Bolsonaro para trabalhar na empresa. *Brasil de Fato*, Brasília, 24 mar. 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: 10 dez. 2023.

NETO, Eduardo Savarese. Computação em Nuvem: O que é, como funciona e importância. *FIA Business School*, 2019. Disponível em: https://fia.com.br/blog/computacao-em-nuvem/. Acesso em: 24 de fev. 2024.

NEVES, Rebeca de Aguilar Pereira. GDPR e LGPD: estudo comparativo. Trabalho de Conclusão de Curso (Bacharel em Direito) – Faculdade de Ciências Jurídicas e Sociais, Centro Universitário de Brasília. Brasília, p. 75, 2021.

ORACLE CORPORATION. Internet of Things. *Oracle*. Disponível em: https://www.oracle.com/br/internet-of-things/. Acesso em: 8 abr. 2025.

ORGANIZAÇÃO PAN-AMERICANA DE SAÚDE (OPAS). Entendendo a infodemia e a desinformação na luta contra a Covid-19. *Kit de ferramentas de transformação digital*. 5p. 2020. Disponível em: https://iris.paho.org/handle/10665.2/52054. Acesso em: 14 de setembro de 2022.

PORTAL G1. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. 28 de janeiro de 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 7 de fevereiro de 2021.

PRIVACY TECH. Governo divulga dados pessoais dos beneficiários do auxílio emergencial e especialistas alertam sobre invasão de privacidade. 9 de junho de 2020. Disponível em: https://www.privacytech.com.br/vazamentos/governo-divulga-dados-pessoais-dos-beneficiarios-do-auxilio-emergencial-e-especialistas-alertam-sobre-invasao-de-privacidade,360518.jhtml . Acesso em: 29 de outubro de 2021.

PYRRHO, M.; BARCELLOS, D. C. B.; CAMBRAIA, L. Flexibilização dos padrões éticos em pesquisa no Brasil: uma análise da Lei 14.874/2024. *Ciência & Saúde Coletiva* [Internet], nov. 2024. Disponível em: http://cienciaesaudecoletiva.com.br/artigos/flexibilizacao-dos-padroes-eticos-em-pesquisa-no-brasil-uma-analise-da-lei-148742024/19426?id=19426&id=19426. Acesso em: 26 mar. 2025.

QUINAGLIA SILVA, Érica; DELMONDES, Júlia Guilherme. A dialética entre o direito à saúde e o direito à proteção de dados pessoais: o poder do Estado na gestão em saúde no Brasil durante a pandemia de Covid-19. In: DUARTE, Aldira Guimarães; AVILA, Carlos F.

Domínguez (Orgs.). *A covid-19 no Brasil: ciência, inovação tecnológica e políticas públicas*. 1ª ed. Curitiba: CRV, 2022, v. 2, p. 267-277.

ROCHA, Bruno Augusto Barros; LIMA, Fernando Rister de Sousa; WALDMAN, Ricardo Libel. Mudanças no papel do indivíduo pós-revolução industrial e o mercado de trabalho na sociedade da informação. *Revista Pensamento Jurídico*, v. 14, n. 1, 2020. Disponível em: https://ojs.unialfa.com.br/index.php/pensamentojuridico/article/view/419. Acesso em: 20 nov. 2023.

SCATOLINI, Lucas. Tenebrosas transações no Ministério da Saúde. *Outras Palavras*, 28 mar. 2022. Disponível em: https://outraspalavras.net/outrasaude/tenebrosas-transacoes-no-ministerio-da-saude/. Acesso em: 27 fev. 2025.

SCHAEFER, Fernanda. Proteção de dados de saúde na sociedade de informação: a busca pelo equilíbrio entre privacidade e interesse social. Curitiba: Juruá Editora, 2010.

SCHWAB, Klaus. A quarta revolução industrial. Edipro, 2019.

SILVEIRA, Sérgio Amadeu; AVELINO, Rodolfo da Silva. Inteligência Artificial, Data Centers e Localização de Dados. In: *ENCONTRO ANUAL DA ANPOCS*, 2023, Campinas. GT Presencial, n. 39. 2023. Disponível em: https://www.encontro2023.anpocs.org.br/trabalho/view?ID_TRABALHO=8023. Acesso em: 24 fev. 2024.

SOCIEDADE BRASILEIRA DE MEDICINA TROPICAL. Revolução da inteligência artificial: uso na saúde traz novas possibilidades. 2023. Disponível em: https://sbmt.org.br/revolucao-da inteligencia-artificial-uso-na-saude-traz-novas-possibilidades/>. Acesso: 24 de fev. 2024.

SOUZA, Joyce. Inteligência Artificial, algoritmos preditivos e o avanço do colonialismo de dados na saúde pública brasileira. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu (Orgs). Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. São Paulo, SP: Autonomia Literária, 2021. cap. 6, p. 107-125.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=P. Acesso em: 12 de setembro de 2022.

UNIVERSIDADE DE SÃO PAULO. Tecnologia da Informação nas Organizações de Saúde, 2015. Disponível em: https://edisciplinas.usp.br/course/view.php?id=7845. Acesso em: 22 nov. 2023.

VERASZTO, Estéfano Vizconde *et al.* Tecnologia: buscando uma definição para o conceito. *Prisma. com*, n. 8, p. 19-46, 2009.

ZUBOFF, Shoshana. A era do capitalismo de vigilância. 1ª ed. Rio de Janeiro: Intrínseca, 2021, 796 p.

Recebido em 23/5/2025 | Aceito em 18/11/2025