ISSN 1809-046X

Revista Estação Científica

Artigo original **DOI: https://doi.org/10.5281/zenodo.14567652**

PROTEÇÃO DE DADOS DOS USUÁRIOS DO APLICATIVO MEU SUS DIGITAL

PROTECTION OF USER'S DATA OF THE APP MEU SUS DIGITAL

Luciana Cristina de Souza[1]

RESUMO

O objetivo do artigo é apresentar os resultados de pesquisa científica a respeito da proteção de informações sensíveis dos usuários do aplicativo Meu SUS Digital e avaliar que medidas têm sido adotadas pelo Poder Público para assegurar os direitos fundamentais dos cidadãos nesse tipo de interação digital. O recorte epistemológico consiste na aplicação do método dialético com enfoque sobre o conceito de Cidades Inteligentes e a necessidade de proteção dos cidadãos que utilizam serviços públicos. Desenvolveu-se pesquisa exploratória e descritiva sobre as tecnologias de arquivamento e salvaguarda das informações dos pacientes tendo por referência normativa a Lei Geral de Proteção de Dados (LGPD). Conclui-se que o ordenamento jurídico brasileiro está em atraso na regulamentação dessas importantes questões de direitos humanos e pode aprender com exemplos de sistemas jurídicos estrangeiros, os quais serão aqui descritos.

PALAVRAS-CHAVE: Cidades inteligentes. Inteligência artificial. Neurodireito. Saúde. Segurança digital.

ABSTRACT

This article aims to present the results of scientific research regarding the protection of user´s sensitive information in the app Meu SUS Digital and assess what measures have been adopted by the Government to ensure the fundamental rights of citizens in

Autor corresponde: Luciana Cristina de Souza, luciana.souza@uemg.br

1 Universidade do Estado de Minas Gerais (UEMG), Belo Horizonte, Minas Gerais, Brasil..

this type of digital interaction. The epistemological approach consists in the application of the phenomenological method focusing on the concept of Smart Cities and the need to protect citizens who use public services. One develop an exploratory and descriptive research on the technologies of archiving and safeguarding of patient information with reference to the General Data Protection Law (LGPD). It is concluded that the Brazilian legal system is lagging in regulating these important human rights issues and can learn from examples of foreign legal systems, which will be described here.

KEYWORDS: Smart Cities. Artificial intelligence. Neurolaw. Health. Digital security.

INTRODUÇÃO

A pesquisa analisou a regulamentação da proteção de dados de saúde no Brasil, a qual se tornou essencial com a implementação das bases de dados digitais, cujos protocolos de segurança precisam ser fortalecidos para assegurar a devida proteção aos usuários. O objetivo era analisar a segurança oferecida pelo aplicativo Conecte SUS, quem em 2024 passou a se chamar Meu SUS Digital, considerando que: a) a modalidade de governo digital está crescendo inegavelmente no país, o que exige que a forma de acesso e os instrumentos de transparência e proteção de dados sejam constantemente atualizados para que a privacidade dos usuários não seja exposta; b) os Municípios são o contato mais próximo com a população quanto o assunto são dados de saúde pública, e vêm buscando se tornar cidades inteligentes, o que exige uma reflexão sobre o que o termo significa na perspectiva dos cidadãos; c) embora o repositório digital do Sistema único de Saúde (SUS) seja de grande porte, ainda há falhas de segurança em alguns momentos e a legislação vigente é insuficiente para regulamentar todos esses incidentes e oferecer uma proteção de melhor qualidade para os usuários do aplicativo.

Nesse cenário de tratamento de informações sobre a saúde, evidentemente um dado sensível, foi proposto na Câmara dos Deputados o Projeto de Lei 522/2022, cujo tema é a inserção da proteção aos neurodireitos na Lei Geral de Proteção de Dados (LGPD) – neurorights – os quais dizem respeito aos direitos subjetivos à

intimidade e à propriedade sobre o próprio corpo (Kellmeyer, 2022; Lopes, 2023). Estes, como outros dados sensíveis sobre saúde, merecem total proteção do poder público, mas, infelizmente, na legislação vigente ainda é insuficiente para oferecer tal garantia aos cidadãos.

Pode ocorrer que uma empresa ou órgão público de posse de dados sensíveis sobre a saúde de uma pessoa busque fazer uso indevido dessa informação. A proteção dos neurodireitos e outras informações pessoais é direito fundamental sobre a personalidade humana (Lopes, 2023). Visando a proteger os pacientes é crucial que políticas públicas de segurança digital sejam promovidas, em especial porque a cada dia mais conteúdo sensível é acrescentado à plataforma governamental. A partir de julho de 2024, além dos dados que já eram registrados, o Meu SUS Digital passou a registrar também a raça dos usuários do sistema público de saúde, bem como seu nome social (Agência Brasil, 2024).

O Programa de Governança em Privacidade do Ministério da Saúde (Ministério da Saúde, 2022) determina a proteção à privacidade desde a concepção e deve perdurar por todas as fases do ciclo de vida dos sistemas de tratamento de dados. Com o intuito de assegurar essa proteção aos usuários do sistema de saúde, os órgãos públicos devem elaborar o Relatório de Impacto à Proteção de Dados Pessoais (Ripd), documento obrigatório no qual deve constar “a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.” (Ministério da Saúde, 2022, p. 15). A Secretaria de Governo Digital também reafirma esse dever em seu Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD), no tópico Boas práticas em segurança da informação (Ministério da Gestão e Inovação em Serviços, 2020, p. 50).

O tema possui relevância na atualidade, uma vez que todos nós temos cada vez mais dados pessoais de natureza sensível arquivados em bancos de informações cujo controle e o nível de transparência ainda estão em construção normativamente. A proteção dos neurodireitos e outros dados sobre saúde urge de ser protegida por uma legislação própria e robusta que regulamente como o conteúdo digital sobre nossas atividades junto aos órgãos de saúde, visto que um grande volume de informações tem sido registrado em exames computadorizados e repositórios digitais,

sendo arquivadas sob o dever de o agente de tratamento de dados assegurar o direito à privacidade, que é personalíssimo.

Se, por um lado, a tecnologia contribui para a análise de grandes volumes de dados de modo a fundamentar melhor a tomada de decisões em políticas públicas, por outro, exige que instrumentos de controle estatal internos e externos sejam desenvolvidos. E que os servidores públicos sejam capacitados ética e tecnologicamente para lidar com as informações de saúde dos cidadãos. Como o Brasil enfrenta na atualidade problemas de integridade e transparência, a vulnerabilidade dos pacientes do SUS é patente. E essa realidade precisa ser alterada para que a gestão municipal de saúde, locus em que se concentram os registros dos pacientes, assuma sua responsabilidade pela guarda e zelo dos dados que registra. A afirmação feita sobre a falta de controle pode ser comprovada consultando-se os indicadores de cumprimento da Agenda 2030 no Brasil, pois se verificará a omissão na coleta de dados relativamente à meta 16.5 desse documento internacional do qual o país é signatário (ODS Brasil, 2023).

Outro exemplo de lacuna legislativa é o projeto de lei sobre o marco legal da inteligência artificial (IA) que ainda está em tramitação o Projeto de Lei do Senado Federal (PLS) 2.338/2023. Em julho de 2024 a tramitação indicava que o mesmo estava sob análise da Comissão Temporária Interna sobre Inteligência Artificial no Brasil da Câmara dos Deputados, que adiou os debates sobre o tema, o que é negativo para a proteção dos direitos fundamentais digitais de privacidade e outros correlatos no país. Somente a União Europeia já publicou norma sobre IA e mesmo esse ato normativo é recente, tendo sido publicado em março de 2024. A preocupação com a segurança e a privacidade no ambiente digital foram debatidas no encontro do G20 Brasil ocorrido em junho de 2024, sendo um dos temas os requisitos de proteção de dados compartilhamento de dados para serviços públicos; no entanto, a inércia legislativa em projetos importantes como PLS 2.338/2023 e PL 522/2022 evidencia um cenário de risco diante do qual a autoridade pública deveria com urgência agir em prol de seus cidadãos.

Verbi gratia, em maio de 2024 um hacker invadiu o sistema do SUS e expôs na Deep web – páginas da internet de difícil identificação e desprovidas de segurança digital – mais de 2 milhões de dados pessoais de usuários do serviço público nacional

de saúde (Security First, 2024). Dados roubados podem ser usados por criminosos e por empresas pouco idôneas no setor de marketing, visto que é uma forma de burlar a necessidade de autorização de sua utilização pelo titular da informação. É um mercado milionário, tanto que em novembro de 2023 foi proposto o PL 234 perante a Câmara dos Deputados com o intuito de criar a Lei de Empoderamento de Dados para deixar mais transparente essa relação entre os usuários e os agentes de tratamento de dados, além de tributar esse crescente setor da economia. Portanto, o debate que essa pesquisa propõe é vital para a garantia da cidadania nas cidades inteligentes, visto que os Municípios estão migrando de modo irreversível para a modalidade de governo digital e isso gerará maior risco de vazamento de dados sensíveis da população se os instrumentos adequados de segurança e privacidade não forem implantados

MÉTODO

O recorte epistemológico foi a aplicação do método dialético com enfoque sobre a gestão pública municipal relativa ao Sistema Único de Saúde (SUS), tendo por base a pesquisa exploratória e descritiva sobre as tecnologias de arquivamento e salvaguarda das informações dos pacientes utilizadas nos últimos dois anos, período em que passou a viger a Lei Geral de Proteção de Dados (LGPD). A pesquisa foi desenvolvida no período 2023-2024. Primeiro foi realizada uma pesquisa descritivo-analítica das obras das Referências que fundamentam esse estudo quanto aos conceitos centrais, tais como: direitos humanos, neurodireitos, direito à privacidade, segurança digital, cidades inteligentes, governança digital, além da Lei Geral de Proteção de Dados.

Em seguida, foi desenvolvido um estudo comparado sob a perspectiva do transconstitucionalismo em relação ao projeto de lei europeu e de nova Constituição do Chile e, tendo por referência, os três projetos de legislação em tramitação no Brasil sobre o tema. Procedeu-se à organização de um quadro normativo e comparativo entre as normas citadas para verificar os dispositivos por elas compartilhados e aqueles que a norma brasileira ainda precisa desenvolver mais com a finalidade de garantir o bem estar da população e um acesso seguro à saúde.

Durante a elaboração do quadro conceitual da pesquisa se esclareceu o significado do termo responsabilidade civil para o estudo comparado, tendo em vista que a principal norma de referência na atualidade é estrangeira, logo, deve-se compreender como esse termo é tratado na literatura externa. Os termos da legislação brasileira anonimização, dados sensíveis, violação de dados e vazamento de informações precisaram ser pesquisados em inglês, sendo seus correspondentes naquele idioma, respectivamente, de-identified data, sensitive covered data, data breach e information leakage.

Como parte da bibliografia está em inglês, é mister esclarecer previamente a grafia do termo responsabilidade nesse idioma: quando significar assumir ônus pela prática de ato ilícito, derivado de culpa aquiliana, o termo em inglês é torts; quando se referir a situações de dever do agente em suas funções ou das partes em um contrato, o termo é liability; e, quando se tratar especificamente de obrigação de prestação de contas oriunda do cargo de gestão, é accountability (Merriam-Webster, 2023). Usa-se comumente a palavra responsabilidade para as três situações no português, todavia, ao pesquisar documentos estrangeiros para a leitura do tema do projeto é imprescindível se atentar para a diferença de terminologias nos artigos estrangeiros, para desse modo aplicar corretamente a teoria no estudo comparado.

Também compôs essa análise o estudo da Carta Brasileira Cidades Inteligentes (2020), documento que determina a inclusão social como um princípio basilar das políticas públicas para implementação de espaços urbanos pautados no uso amplo da tecnologia digital pela população acessar serviços públicos, dentre outras diretrizes. Foi feita a leitura crítica dos documentos para categorização dos valores mais relevantes nas Cidades Inteligentes para contrastar com os indicadores da NBR ISO 37122 tendo por referência de análise o modelo de desenvolvimento da Constituição da República de 1988 e da Agenda 2030, cujo foco é assegurar que a questão econômica nos debates sobre tecnologia digital não sirva para privar os usuários dos sistemas de seus direitos fundamentais.

RESULTADOS E DISCUSSÃO

Após os meses dedicado à pesquisa, observou-se que:

I - Quanto à gestão de cidades inteligentes:

Os Municípios buscam ser certificados como cidades inteligentes por informatizarem o funcionamento de serviços públicos, contudo, sem compreender que o termo depende de outros requisitos para ser alcançado e envolve mais do que apenas adquirir aparato tecnológico; também diz respeito à segurança digital. O termo "inteligente" não é apenas referência ao uso de instrumentos digitais, como também de boa governança pública quanto às escolhas feitas visando a sustentabilidade da vida humana e sua dignidade nos espaços urbanos. Uma cidade high-tech com baixo Índice de Desenvolvimento Humanos (IDH), por exemplo, não pode ser realmente validada, visto que coloca o bem estar dos seus cidadãos em segundo lugar frente aos investimentos destinados para parques tecnológicos e a área econômica, como se vê a seguir:

Art. 5º As políticas públicas relativas à inclusão digital objetivam ainda:

I - fomentar e implantar a infraestrutura, os serviços, os sistemas e as aplicações baseados em TIC, necessários para o acesso às redes de telecomunicações pela população:

a) de localidades remotas;

b) de localidades com prestação inadequada ou inexistente desses serviços; ou

c) em situação de vulnerabilidade social

(Brasil, Decreto 9.612/2018)

Essa preocupação está presente na Agenda 2030 e na Carta Brasileira de Cidades Inteligentes:

ODS 9, meta 9.c: Aumentar significativamente o acesso às tecnologias de informação e comunicação e empenhar-se para procurar ao máximo oferecer acesso universal e a preços acessíveis à internet nos países menos desenvolvidos, até 2020.

(...)

ODS 11: Tornar as cidades e os assentamentos humanos inclusivos, seguros, resilientes e sustentáveis

(Organização das Nações Unidas, 2015)

CIDADES INTELIGENTES São cidades comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação. (Brasil, 2020, p. 28-29)

Como se infere das normas citadas, é crucial defender-se o equilíbrio da tríade social-econômico-tecnológico para promover um modelo democrático e protetivo de desenvolvimento da saúde pública municipal, prática que se coaduna com direito disposto na Constituição Federal de 1988: “Art. 182. A política de desenvolvimento urbano, executada pelo Poder Público municipal, conforme diretrizes gerais fixadas em lei, tem por objetivo ordenar o pleno desenvolvimento das funções sociais da cidade e garantir o bem-estar de seus habitantes.”

Uma das formas possíveis de exercer esse controle é a correta aplicação da NBR ISO 37122. Essa norma técnica é uma certificação a ser aplicada para monitorar o processo de elaboração e de execução de políticas públicas voltadas à implantação de cidades inteligentes por meio de um conjunto de indicadores distribuídos em 19 áreas temáticas, sendo um deles sobre saúde pública. Esses indicadores precisam ser construídos e avaliados pelo poder público em parceria com a sociedade com vistas a garantir a transparência no tratamento dos dados sensíveis. A participação popular no processo de tomada de decisões sobre políticas públicas nas cidades, certificadas ou não como “inteligentes”, deriva da Constituição da República de 1988, que dispõe a respeito da soberania popular no parágrafo único do Art. 1º.

II - Quanto à necessidade de regulação da proteção de dados:

A preocupação com dados sensíveis sobre a saúde é relevante não somente no Brasil. O Projeto de Lei 522/22 da Câmara dos Deputados, como dito, pretende

inserir esse nível de proteção à atual Lei Geral de Proteção de Dados de modo a assegurar maior segurança digital para os cidadãos. E, dada a relevância do tema na atualidade, é que se propôs essa investigação científica para analisar a política de privacidade do aplicativo Conecte SUS, atualmente Meu SUS Digital, pois esta é uma seara em que novas normas e políticas públicas se tornarão cada vez mais significativas para proteger os direitos subjetivos fundamentais, inclusive de dados sobre a saúde e o perfil dos usuários desse sistema. Em reunião realizada em janeiro de 2024, o Conselho Nacional de Saúde se manifestou no sentido de o poder público exercer melhor controle com “a segurança dos dados, considerando que houve um período de ataques de hackers no site do Ministério da Saúde-MS e vazamento de dados de usuários” (Ministério da Saúde, 2024), cenário vantajoso que o documento aponta que poderá ser alcançado se houver maior participação social e transparência na integração e gestão dos sistemas aos quais o aplicativo se conecta.

Observou-se que essa preocupação se justifica tendo em vista que ainda acontecem incidentes de falha na segurança de dados do sistema de saúde público. A título de exemplos, havendo outros casos que poderiam ser citados, em 2002 o Sistema Único de Saúde foi autuado por causa de vazamento de dados de milhões de usuários e, ano passado, também foi autuada a Secretaria de Estado da Saúde de Santa Catarina (Agência Nacional de Proteção de Dados, 2022; 2023).

Com o intuito de auxiliar o processo de implementação tecnológica pelos serviços públicos na modalidade de governo digital, a Agência Nacional de Proteção de Dados (ANPD) criou um sandbox regulatório visando a “facilitar a inovação dentro de uma estrutura sujeita à regulação” e instituir instrumentos normativos para a supervisão dos experimentos e testes tecnológicos, assim protegendo os direitos dos usuários desses novos sistemas (p. 10). Para funcionar, essa metodologia exige a colaboração do governo, das entidades privadas e da sociedade civil. A necessidade de um ambiente controlado para a gradativa testagem e implementação de novas tecnologias decorre do fato de que os impactos negativos no seu uso atingem sempre larga escala, são milhões de usuários atingidos simultaneamente e a reparação do erro é sempre cara e extremamente difícil – vide exemplo a divulgação de fotos íntimas na internet, cujas vítimas continuamente convivem com as postagens. A

criação de marcos regulatórios é imprescindível para que se possa garantir a dignidade da pessoa humana (Barcellos, 2011).

Para as empresas de tecnologia e marketing que lucram com a venda de dados pessoais, a regulação é vista como inimiga e comumente se invoca a desculpa de que prejudica a inovação. Na verdade, o que defendem não é o caráter inovador dos recursos digitais, mas a preservação de seu modo predatório de lucro independente do prejuízo que causam às vítimas do vazamento de dados. Também se opõem ao requisito de anuência do titular da informação, porque passariam a ter que efetivamente informar como obtém ganhos com a vida pessoa de outras pessoas e se responsabilizar pela divulgação indevida desses dados. No entanto, é vital compreender que o conceito de mercado livre é diferente de desregulação ou anarquia. Exemplo disso é que se nenhuma regulação fosse permitida quanto ao direito de propriedade, patentes não existiriam e as pessoas não teriam como defender seus domicílios em caso de turbação. Dados pessoais também são propriedade privada e, como tal, merecem a mesma proteção que todos os bens e posses que o ser humano detém. Quando uma empresa coleta e usa essa informação sem autorização expressa obtida de modo idôneo, está ferindo frontalmente o direito de propriedade privada, não somente os direitos personalíssimos dos indivíduos.

Logo, é essencial a supervisão desses processos de inovação, como em sua origem pretendia o PLS 2.338/2023, conquanto o forte lobby das Big Techs pressione pela desregulamentação com o discurso falacioso de uma suposta justificativa de ser em prol da inovação – nesse sentido foram propostas diversas emendas ao texto original em junho de 2024. Inovação por si só não justifica tudo; exemplo disso é que o tráfico de drogas está sempre atingindo os jovens com produtos novos, mas continua praticando crime. O ato de inovar, para ser legal, deve estar balizado pelos seguintes princípios: a) a inovação não pode ferir direito já existente e tampouco constituir facilitação à prática de delito (civil, criminal, ambiental, etc.); b) é obrigatória a supervisão democrática dos avanços tecnológicos para evitar discriminações e o lobismo que possam prejudicar o equilíbrio na sociedade; c) os testes da inovação precisam primeiro passar por um sandbox regulatório. Além disso, o Estado brasileiro deve se comprometer com a efetivação das normas previstas no PL 522/2022, PL

234/2023 e PLS 2.338/2023, visto que sem a fruição da norma na vida concreta, sua previsão apenas in abstrato a torna inócua (Barcellos, 2011, p. 107).

III - Quanto ao que dizem os sistemas estrangeiros:

O Brasil pode aprender com o debate que vem sendo promovido em outros países. Verbi gratia, o atual projeto de Constituição para o Chile (UCAMPUS, 2023) acrescentará ao ordenamento jurídico daquele país novos dispositivos de proteção para os indivíduos que seriam também tratariam positiva contribuição para o ordenamento jurídico brasileiro. Como a proposta de 2019, por outras razões, foi rejeitada no plebiscito nacional, em 2021, o Poder Legislativo chileno optou por fazer uma emenda constitucional no texto vigente para que a proteção de dados já pudesse ser implementada enquanto o país não promulga a nova Constituição.

El desarrollo científico y tecnológico estará al servicio de las personas y se llevará a cabo con respeto a la vida y a la integridad física y psíquica. La ley regulará los requisitos, condiciones y restricciones para su utilización en las personas, debiendo resguardar especialmente la actividad cerebral, así como la información proveniente de ella. (Chile, Ley 21.383/2021, artigo único)

A proposta chilena segue o mesmo caminho que tem sido debatido na União Europeia, haja vista a Ley Orgánica 3/2018, da Espanha, que trata da Protección de Datos Personales y garantía de los derechos digitales, assim como o Artificial Intelligence Act da União Europeia, que é a primeira norma reguladora de inteligência artificial do mundo e somente entrou em vigor em março de 2024. Em diversos países a aprovação do sandbox regulatório sofre grande pressão de empresas privadas de tecnologia contrárias à regulamentação, tal como ocorreu com a LGPD brasileira, publicada em 2018, que teve prorrogação de sua vacatio legis, inclusive.

Nos Estados Unidos da América, país sede da maioria das Big Techs que atuam no Brasil – por exemplo, Google, Microsoft, Apple, Meta, Tesla e Oracle – apenas dez dos cinquenta estados conseguiram aprovar normas regulatórias. Isso ocorre porque a norma de âmbito nacional, a American Data Privacy and Protection Act (ADPPA), aprovada apenas em 2022 e com muita oposição interna, define na cláusula 32 que serão os estados-membros os detentores do direito de organizar uma

State privacy authority, fragmentando o arcabouço jurídico de proteção dos dados sensíveis. É nitidamente observável que o lobby contra uma maior proteção dos direitos individuais no setor digital tem sido um grande obstáculo ao desenvolvimento de uma sandbox regulatória que proteja os cidadãos naquele país.

Porém, o aperfeiçoamento da legislação poderia contribuir no combate ao data breach / information linkage, uma vez que existiria um controle mais eficaz contra abusos praticados pelas empresas de tecnologia e marketing, bem como otimizando os instrumentos de segurança digital, muito necessários. Por exemplo, em fevereiro de 2024, um ciberataque vazou um imenso número de dados sensíveis sobre saúde nos Estados Unidos (Twingate, 2024; UnitedHealth Group, 2024). O incidente atingiu o serviço público e o um importante parceiro privado com milhões de usuários, o qual atua junto a hospitais particulares e a órgãos governamentais, o Change Healthcare (2024). Quanto a ocorrido, revela a premência de legislação robusta sobre proteção de dados de saúde, atualizando para Era Digital o escopo de normas como o Health Insurance Portability and Accountability Act (1996).

> [...] a HIPAA é uma norma norte-americana que aprofunda questões técnicas de infraestrutura que a LGPD, lei brasileira, não aborda. Assim, ambas devem ser consideradas complementares, sendo a norma HIPAA uma forma para atender à LGPD com ainda mais segurança técnica.
>
> [...]
>
> ao focar em confidencialidade, integridade e disponibilidade das informações de saúde, a norma HIPAA valoriza os três pilares principais da segurança da informação.

Logo, seria significativo para os projetos de lei brasileiros considerarem, como a HIPAA, os pilares do compliance, pois um rigoroso controle de integridade oferecerá melhores garantias contra vazamento de dados. A parâmetro internacional COSO 2017 (Gestão de Riscos) já foi adotado no Brasil (Tribunal de Contas da União, 2024) e, infelizmente, sua implantação tem sido lenta. Prova disso é que não há indicadores brasileiros sobre a variável 16.6.2 - Proporção da população satisfeita com a última experiência com serviços públicos, da meta 16.6 - Desenvolver instituições eficazes,

responsáveis e transparentes em todos os níveis, do ODS 16, da Agenda 2030, que avalia o grau de responsabilidade das instituições (ODS Brasil, 2024). A adoção mais efetiva dessas normas técnicas de controle de integridade aplicadas em conjunto com a LGPD e a aprovação dos projetos de lei em tramitação que foram aqui citados é vital no cenário de desrespeito e ofensas à privacidade que se observa.

CONSIDERAÇÕES FINAIS

Nesse cenário em que as cidades migram rapidamente para a gestão tecnológica dos serviços públicos, inclusive os de saúde, a sandbox regulatória é uma questão primordial para a proteção de dados, sendo papel do Estado Democrático de Direito debater com seus cidadãos sobre o modelo de governança a ser adotado atualmente, já que não é opcional fazer parte da modalidade de governo digital. A Constituição da República de 1988 oferece às cidadãs e aos cidadãos instrumentos para a defesa de direitos considerados relevantes para organização da vida nas cidades, os quais fazem da política urbana brasileira. Essa engloba uma séria de políticas públicas e de legislações aplicáveis à regulamentação das relações sociais que atualmente dependem em grande parte do uso de tecnologias digitais.

Igualmente, compete aos Municípios buscar equilibrar a tríade tecnologia – economia – social para assegurar que: a) todas as pessoas sejam incluídas nas cidades inteligentes e no governo digital; b) o intenso volume de informações sensíveis que os serviços públicos digitais acumulam sejam protegidos devidamente para proteção dos cidadãos. Isso significa que é imprescindível maior participação da sociedade civil nos debates a respeito de três propostas de legislação essenciais para o momento: PL 522/2022, PLS 2.338/2023, PL 234/2023, os quais devem ser aprovados o mais rapidamente possível diante do risco de vazamento de dados para a Deep web e outros incidentes de segurança que possam ocorrer.

Em suma, é vital desenvolver a modalidade de governo digital e das cidades inteligentes considerando a crescente necessidade de contínuas atualizações de sistemas para garantir que os instrumentos de transparência e proteção de dados sejam capazes de prover privacidade aos usuários. Além disso, democratizar o debate com a sociedade civil poderá contribuir para maior celeridade na aprovação

das normas necessárias e equilibrará a vontade dos cidadãos com om contante lobby que as Big Techs exercem sobre o Congresso Nacional. No caso das cidades inteligentes, significa implementar políticas públicas de inclusão digital e de proteção para os usuários dos serviços públicos na modalidade de governo digital tendo por paradigma a democracia participativa e deliberativa prevista no texto constitucional, de modo que os cidadãos tenham meios concretos para defender suas liberdades civis, entre elas a privacidade.

REFERÊNCIAS

AGÊNCIA BRASIL. **Aplicativo do SUS passa a aceitar dados sobre raça e nome social**. Saúde, Notícias, 08 de julho de 2024. Disponível em: https://agenciabrasil.ebc.com.br/saude/noticia/2024-07/aplicativo-do-sus-passa-aceitar-dados-sobre-raca-e-nome-social#:~:text=A%20partir%20desta%20segunda%2Dfeira,b%C3%A1sicas%20de%20sa%C3%BAde%20(UBSs). Acesso em 08 de julho de 2024.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Relatório de Instrução Nº 4/2023/FIS/CGF/ANPD**. Autuado: Secretaria de Estado da Saúde de Santa Catarina. Processo nº 00261.001886/2022-51, 11 de outubro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-incidente-ao-site-do-conectsus Acesso em 28 de junho de 2024.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **Sandbox Regulatório de Inteligência Artificial e Proteção de Dados no Brasil**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-prorroga-consulta-a-sociedade-sobre-sandbox-regulatorio-ate-1o-de-dezembro Acesso em 28 de junho de 2024.

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. **ANPD fiscaliza incidente do Ministério da Saúde e Conecte SUS**. Notícias, 31 de outubro de 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-incidente-ao-site-do-conectsus Acesso em 28 de junho de 2024.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS – ABNT. **NBR ISO 37122: Cidades e Comunidades Sustentáveis – Indicadores para Cidades Inteligentes**. São Paulo: ABNT: 24 de junho de 2021.

BARCELLOS, Ana Paula de. **A eficácia jurídica dos princípios constitucionais**. 3ed. São Paulo: Renovar, 2011.

BRASIL. Constituição da República Federativa do Brasil, promulgada 05 de outubro de 1988. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 28 de junho de 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Brasília: Senado Federal, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 28 de maio de 2024.

BRASIL. Ministério do Desenvolvimento Regional. **Carta Brasileira Cidades Inteligentes**. Brasília, 2020. Disponível em: <https://www.gov.br/mdr/pt-br/assuntos/desenvolvimento-regional/projeto-andus/carta_brasileira_cidades_inteligentes.pdf >. Acesso em 21 jan. 2024.

BRASIL. **Decreto 9.612, de 17 de dezembro de 2018**. Dispõe sobre políticas públicas de telecomunicações. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9612.htm>. Acesso em 09 jan. 2024.

CÂMARA DOS DEPUTADOS. **Projeto de Lei 234, de 11 de novembro de 2023**. Institui a Lei Geral de Empoderamento de Dados, dispõe sobre o Ecossistema Brasileiro de Monetização de Dados, altera a Lei Complementar nº 111, de 6 de julho de 2001, e as Leis nº 10.406, de 10 de janeiro de 2002, nº 10.833, de 29 de dezembro de 200, nº 12.965, de 23 de abril de 2014, e nº 13.709, de 14 de agosto de 2018, e dá outras providências. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2401133 Acesso em 10 de julho de 2024.

CÂMARA DOS DEPUTADOS. **Projeto de Lei 522, de 09 de março de 2022**. Modifica a Lei n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), a fim de conceituar dado neural e regulamentar a sua proteção. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2317524 Acesso em 10 de junho de 2024.

CHANGE HEALTCARE. **HIPAA website substitute notice - Notice of data breach**. Disponível em: https://www.changehealthcare.com/hipaa-substitute-notice Acesso em 25 de junho de 2024.

CHILE. Biblioteca del Congreso Nacional del Chile. **Ley 21383 - Modifica la Carta Fundamental, para establecer el desarrollo científico y tecnológico al servicio de las personas (2021)**. Disponível em: https://www.bcn.cl/leychile/navegar?idNorma=1166983 Acesso em 20 de junho de 2024.

CHILE. **Propuesta de Constitución Política de la República de Chile (2019)**. Disponível em: https://www.procesoconstitucional.cl/docs/Propuesta-Nueva-Constitucion.pdf Acesso em 20 de junho de 2024.

COSO - COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Enterprise risk management integrating with strategy and performance**. [S.l.]: COSO, 2017. Disponível em: https://www.coso.org/guidance-erm Acesso em 27 de junho de 2024.

ESPANHA. **Ley Orgánica 3, de 5 de diciembre de 2018**. Protección de Datos Personales y garantía de los derechos digitales. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673 Acesso em 22 de março de 2024.

EUROPEAN PARLIAMENT. **Artificial Intelligence Act**. European Parliament, 13 March 2024. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf. Acesso em 22 de março de 2024.

G20 BRASIL. **Portal brasileiro Gov.br é destaque global no workshop de Governo Digital e Inclusão**. Disponível em: https://www.g20.org/pt-br/noticias/portal-brasileiro-gov-br-e-destaque-global-no-workshop-de-governo-digital-e-inclusao Acesso em 22 de junho de 2024.

HIPAA: o que é e porque seguir este modelo? **FlowTI**, Blog, Segurança da Informação, 03 de agosto de 2023. Disponível em: https://flowti.com.br/blog/hipaa-o-que-e-e-porque-seguir-este-modelo Acesso em 27 de junho de 2024.

KELLMEYER, Philipp. *Neurorights* - A Human Rights–Based Approach for Governing Neurotechnologies. In: VOENEKY, Silja *et al.* **The Cambridge Handbook of Responsible Artificial Intelligence Interdisciplinary Perspectives**. Part VII - Responsible AI Healthcare and Neurotechnology Governance, Cap. 24, p. 412-426, outubro de 2022. Disponível em: https://www.cambridge.org/core/books/cambridge-handbook-of-responsible-artificialintelligence/*neurorights*/AF85DE57D51D114E26C19146E234F897. Acesso em 13 de junho de 2024.

LOPES, Ana Maria D'Ávila et al (Org.). **Neurodireito, neurotecnologia e direitos humanos**. Porto Alegre: Livraria do Advogado, 2023.

MERRIAM-WEBSTER. *Law Dictionary*. Disponível em: https://www.merriam-webster.com/legal. Acesso em 15 de junho de 2023.

MEU SUS DIGITAL. Plataforma do Ministério da Saúde. **Novo aplicativo substitui o Conecte SUS; saiba como utilizá-lo**. Notícias, 23 de fevereiro de 2024. Disponível em: https://meususdigital.com/novo-aplicativo-substitui-o-conecte-sus-saiba-como-utiliza-lo/. Acesso em 12 de março de 2024.

MINISTÉRIO DA GESTÃO E INOVAÇÃO EM SERVIÇOS. Secretaria de Governo Digital. **Guia de boas práticas - Lei Geral de Proteção de Dados (LGPD)**. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em 14 de junho de 2024.

MINISTÉRIO DA SAÚDE. Comitê Executivo de Tecnologia da Informação e Comunicação. **Ata 2ª Reunião Ordinária do CETIC/MS - 24/01/2024**. Brasília: Ministério da Saúde - Assessoria Especial de Proteção de Dados, 2022. Disponível em: https://datasus.saude.gov.br/wp-content/uploads/2024/02/SEI_MS-0038796386-Ata-CETIC-24-01.pdf Acesso em 17 de junho de 2024.

MINISTÉRIO DA SAÚDE. **Programa de Governança em Privacidade**. Brasília: Ministério da Saúde - Assessoria Especial de Proteção de Dados, 2022. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em 17 de junho de 2024.

MINISTÉRIO DA SAÚDE. Secretaria-Executiva. Departamento de Informática do SUS. **Estratégia de Saúde Digital para o Brasil 2020-2028**. Brasília: Ministério da Saúde, 2020.

ODS BRASIL. **Agenda 2030:** Indicadores Brasileiros para os Objetivos de Desenvolvimento Sustentável. Disponível em: https://odsbrasil.gov.br Acesso em 21 de junho de 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS - ONU. **Agenda 2030**. Nova York: UN, 2015. Disponível em: https://www.undp.org/content/dam/brazil/docs/agenda2030/undp-br-Agenda2030-completopt-br-2016.pdf. Acesso em 20 de maio de 2024.

SECURITY FIRST. **Hacker invade o SUS e expõe dados de 2 milhões de usuários na DeepWeb**. Notícias, 23 de maio de 2024. Disponível em: https://securityfirst.com.br/hacker-invade-o-sus-e-expoe-dados-de-2-milhoes-de-usuarios-na-deepweb/ Acesso em 14 de junho de 2024.

SENADO FEDERAL. **Projeto de Lei 2.338, de 03 de maio de 2023**. Marco Legal da Inteligência Artificial no Brasil. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233Acesso em 10 de julho de 2024.

TWINGATE. **United Healthcare Data Breach: What & How It Happened?** Blog, junho de 2024. Disponível em: https://www.twingate.com/blog/tips/United%20Healthcare-data-breach Acesso em 25 de junho de 2024.

TRIBUNAL DE CONTAS DA UNIÃO. **Modelos de referência de gestão corporativa de riscos**. Portal TCU, Gestão de Riscos, 2024. Disponível em: https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/politica-de-gestao-de-riscos/modelos-de-referencia.htm#:~:text=O%20COSO%2DERM%20introduz%20conceitos,alcance%20de%20um%20certo%20objetivo Acesso em 27 de junho de 2024.

UCAMPUS. Secretaría de Participación Ciudadana. **Proyecto de Constitución**. Chile, 2023. Disponível em:

https://ucampus.quieroparticipar.cl/m/iniciativas/anteproyecto?cap_id=2. Acesso em 25 de junho de 2024.

UNITEDHEALTH GROUP. **Information on the Change Healthcare Cyber Response**. Disponível em: https://www.unitedhealthgroup.com/ns/changehealthcare.html Acesso em 25 de junho de 2024.

UNITED STATES. Congress. **American Data Privacy and Protection Act**. Disponível em: https://www.congress.gov/bill/117th-congress/house-bill/8152/all-actions?overview=closed#tabs Acesso em 25 de junho de 2024.

UNITED STATES. Congress. **Health Insurance Portability and Accountability Act**. Disponível em: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf Acesso em 25 de junho de 2024.
.

Apoio financeiro: Bolsa de Produtividade PQ/UEMG – Edital 6/2023.