

**PROTEÇÃO DOS DADOS PESSOAIS NA REALIDADE VIRTUAL:
PONDERAÇÕES SOBRE O META® NA ÉGIDE DO
CONSTITUCIONALISMO DIGITAL**

PROTECTION OF PERSONAL DATA IN VIRTUAL REALITY:
CONSIDERATIONS ON META® IN THE AEGIS OF DIGITAL
CONSTITUTIONALISM

Caroline de Carvalho Leitão Hidd¹

Sebastiao Patrício Mendes da Costa²

RESUMO: O mundo se torna cada vez mais conectado e as tecnologias imersivas ganham um espaço mais amplo no governo, nas empresas e no mercado de consumo, sendo necessária uma estrutura de segurança e privacidade para regulamentá-las. O Meta, nessa conjuntura, representa um novo paradigma, apontado por alguns como a próxima fase da evolução humana. Nessa ferramenta, os corpos físicos são projetados na forma de avatares em um mundo virtual semelhante à forma como se percebe o próprio mundo real. Como objetivo geral, a pesquisa tenciona estudar os desafios enfrentados pelo direito constitucional digital, no âmbito das tecnologias de realidade virtual. Empregou-se o método hipotético-dedutivo de abordagem e fez-se uso de uma pesquisa majoritariamente bibliográfica e documental, lastreada na Constituição brasileira de 1988, no Marco Civil da Internet (Lei 12.965/2014), na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e em uma variada gama de autores; tais como Hoffmann-Riem (2020), Sarlet (2020) e Cameron e Pearlman (2022). Ao final, conclui-se ser necessário definir um regime de responsabilidade civil pelo conteúdo veiculado nessas redes, embora a concepção, a criação e a implementação de tal regime seja difícil, tendo em vista a previsibilidade limitada do desenvolvimento futuro da digitalização e seus problemas subsequentes.

¹ Auditora de controle externo do TCE/PI. Especialista em Direito constitucional e Controle na Administração Pública pela UFPI. Mestranda em Direito pela UFPI. E-mail: carolinecleitao@hotmail.com. Lattes: <http://lattes.cnpq.br/0805320905723406>.

² Pós-doutorado em Direito Civil e Filosofia do Direito pela Universität Augsburg (Alemanha). Doutor em Direito pela PUC/RS. Mestre em Direito e Estado pela UnB. Mestre em Antropologia e Arqueologia pela UFPI. Professor do curso de graduação e mestrado em Direito da UFPI. E-mail: sebastiaocosta@ufpi.edu.br. Lattes: <http://lattes.cnpq.br/6810023102929766>.

Palavras-chave: Constitucionalismo digital; Meta; Proteção de dados pessoais; Realidade virtual.

ABSTRACT: As the world becomes increasingly connected and immersive technologies gain a larger space in government, businesses and the consumer market, a security and privacy structure is needed to regulate them. Meta, at this juncture, represents a new paradigm, pointed by some as the next phase of human evolution. In this tool, the physical bodies are projected in the form of avatars in a virtual world similar to how it is perceived or the real world itself. As a general objective, the research aims to study the challenges faced by digital constitutional law, in the field of virtual reality technologies. The hypothetical-deductive method of approach was employed and the use of a mostly bibliographical and documentary research was used, weighed down by the Brazilian Constitution of 1988, not the Civil Framework of the Internet (Lei 12.965/2014), in the Geral Law for the Protection of People's Data (Law no. 13,709/2018) and in a wide range of authors related to the fundamental rights and use of the internet, such as Hoffmann-Riem (2020), Sarlet (2020), Cameron and Pearlman (2022). In the end, the conclusion was that it would be necessary to define a civil liability regime for the content conveyed in these networks, but the conception, creation and implementation of such a regime would be difficult, in view of the limited predictability of the future development of digitization and its subsequent problems.

Keywords: Digital Constitutionalism; Meta; Protection of personal data; Virtual reality.

1 INTRODUÇÃO

Há, no presente momento, um movimento de convergência do mundo “real” para o digital, em que as relações sociais, trabalhistas, acadêmicas, científicas e políticas estão se convertendo, de alguma forma, para o mundo digital. Logicamente, houve a intensificação da virtualização em decorrência da pandemia da Covid-19, o que acelerou todo o processo de uso do ambiente digital para realizar atividades diárias, como reuniões através dos aplicativos “Zoom” e “Google Meetings”.

Em outubro de 2021, um dos fundadores do Facebook, Mark Zuckerberg, anunciou que a empresa passaria a se chamar “Meta”, o que popularizou o termo “metaverso”. O objetivo da “nova” empresa é formular um conjunto de *software* e *hardware* que permitirá replicar todas as interações humanas do dia a dia, indo do trabalho às atividades recreativas sociais, servindo a uma experiência imersiva e multissensorial

que impossibilitaria a diferenciação entre a realidade e o mundo virtual. Conseqüentemente, com essa projeção da pessoa para o mundo virtual haverá, também, a projeção quanto aos direitos da personalidade do mundo real.

Contudo, mesmo com o Marco Civil da Internet – MCI e a Lei Geral de Proteção de Dados – LGPD, as redes sociais, os aplicativos e os sites ainda não possuem uma política clara sobre como será o tratamento dos dados pessoais nesses sistemas de realidade alternativa, apesar de, a todo momento, os “passos” do usuário da internet serem monitorados e registrados, como uma forma de mineração e captação de dados, colocando em xeque a questão da proteção dos dados pessoais.

Frente ao cenário proposto, a presente pesquisa tem como alicerce o seguinte problema: a partir do ponto de vista do constitucionalismo digital, quais os desafios enfrentados no metaverso, mais especificamente no Meta, para a proteção dos dados pessoais? Sendo assim, em linha de hipótese de pesquisa, estabelece-se a seguinte proposição: a legislação brasileira, apesar de abordar a questão dos dados pessoais digitais, precisa avançar exponencialmente para que possa acompanhar a rápida evolução do metaverso.

Neste sentido, o debate acadêmico se mostra ferramenta de extrema relevância e pode trazer luz a esta importante tarefa incumbida aos operadores do Direito, que, mesmo diante da falta de clareza e complexidade de circunscrição entre o real e o virtual, não podem deixar de dar respostas a situações concretas que já começam a impactar o dia a dia dos cidadãos.

Como objetivo geral, a pesquisa tenciona estudar os desafios enfrentados pelo direito constitucional digital, no âmbito das tecnologias de realidade virtual, enquanto os objetivos específicos são tecidos nas seguintes estruturas: (i) analisar o surgimento e o objeto de estudo do constitucionalismo digital; (ii) compreender o funcionamento e o impacto do Meta nas tecnologias da informação; e, por fim, (iii) realizar ponderações acerca da proteção dos dados pessoais no âmbito do metaverso.

No que tange à metodologia, emprega-se o método hipotético-dedutivo de abordagem, uma vez que se estabelece como linha diretriz que o direito de proteção dos

dados pessoais, no cenário jurídico-constitucional brasileiro, tem sua aplicação garantida no mundo real, mas, ao compreender que a realidade virtual seria uma extensão da realidade fática, necessitar-se-ia uma reinterpretação desse direito para adequar-se às novas circunstâncias. Evidentemente, a pesquisa é bibliográfica e documental, porquanto é lastreada, além da Constituição brasileira de 1988, no Marco Civil da Internet (Lei 12.965/2014), na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e em uma variada gama de autores atinentes aos direitos fundamentais e ao uso da internet, a partir de diálogos e contraposições para uma posição consentânea ao problema proposto.

Para atingir os objetivos, dividiu-se a pesquisa em três seções: a primeira seção buscou compreender como o desenvolvimento histórico da internet repercutiu no surgimento do constitucionalismo digital, apontando seu objeto de estudo e suas preocupações. Na segunda seção, analisou-se como se dá a proteção dos dados pessoais em ambientes virtuais, apontando, inclusive, a legislação pátria sobre o tema. Por fim, na terceira seção, realizou-se ponderações sobre a criação do metaverso denominado Meta, discutindo as implicações desse sistema para os direitos fundamentais.

2 O QUE É CONSTITUCIONALISMO DIGITAL?

Desde o seu surgimento, a tecnologia – mais especificamente aquela relacionada à informação e à comunicação – resultou em uma profunda transformação da sociedade, repercutindo em uma mudança substancial nas condições de vida, seja no âmbito governamental/industrial seja transformando os hábitos sociais.

Evidenciando o plano social, Hoffmann-Riem (2020) pontua que os algoritmos digitais têm sido utilizados até mesmo para influenciar atitudes, valores e comportamentos; podendo, inclusive, influir em processos de tomada de decisão. O desenvolvimento histórico da *internet* mostra que, em sua fase inicial, ela foi recebida por muitos como um novo meio de desenvolvimento livre. Contudo, mediante uma conjuntura de constante mudança, a evolução da tecnologia tem imposto desafios para o

direito, que passa, na visão de Fritz e Mendes (2019), a deparar-se frequentemente com situações inéditas ou ainda pouco vivenciadas, necessitando de regulação.

Lima e Costa (2019, p. 174) retratam a relação basilar entre a inovação e o direito, na medida em que “a ciência passa a ser lida como (...) compromisso dessa nova sociedade com a inovação, que começa a ser objeto de regulação jurídica, bem como parâmetro para a produção do direito”. Desse modo, tem-se o Direito Constitucional como disciplina elementar, haja vista ser um modelo universal de organização e legitimação, responsável por guiar a elaboração e aplicação do ordenamento jurídico como um todo. Segundo Mendes e Fernandes (2020), a expressão constitucionalismo digital, inicialmente, referenciava uma ideologia que defendia a limitação do poder dos atores privados no meio digital em contraposição à ideia de limitação do poder político estatal.

Posteriormente, a expressão passou a ser utilizada de forma mais abrangente, abarcando quaisquer iniciativas (jurídicas ou não, estatais ou não) que tivessem por objeto a afirmação dos direitos fundamentais na *internet*, uma espécie de “declaração dos direitos fundamentais” no âmbito digital. Todavia, para os autores, o constitucionalismo digital seria simplesmente uma “corrente teórica do Direito Constitucional contemporâneo que se organiza a partir de prescrições normativas comuns de reconhecimento, afirmação e proteção de direitos fundamentais no ciberespaço” (MENDES; FERNANDES, 2020, p. 05), acreditando que tais direitos podem ser usufruídos por seus titulares sem a necessária exclusão regulatória do Estado, uma vez que é plenamente possível que este atue ao lado de agentes privados.

Celeste (2019) explica que o advento da tecnologia digital teria alterado o ecossistema constitucional em alguns aspectos, que envolvem, basicamente, a proteção de direitos fundamentais e o equilíbrio entre poderes. Em relação ao tema dos direitos fundamentais, o autor afirma que a tecnologia foi responsável por amplificar as possibilidades de os indivíduos exercerem os seus direitos fundamentais, tais como os direitos de liberdade de expressão, de liberdade religiosa, de liberdade de reunião etc., já que aquela expande a possibilidade de transmissão da informação. Em contrapartida, a

tecnologia aumentou o risco de ameaças aos direitos fundamentais. A difamação, o discurso de ódio, o *cyberbullying* e a pornografia infantil são apenas alguns exemplos de como a liberdade de expressão pode ser levada ao extremo através dos meios digitais.

Embora a modernidade digital tenha trazido inúmeros benefícios à sociedade, é inegável que aquela pode: bloquear ou limitar a transmissão da informação; controlar o conteúdo da transmissão da informação; e registrar outras informações relacionadas com os indivíduos envolvidos na informação transmitida. A questão é que uma limitação da transmissão da informação poderia violar todos os direitos que se baseiam nessa transmissão, tais como a liberdade de expressão, a liberdade de informação, a liberdade de associação etc.

Quanto ao controle do conteúdo da transmissão, a informação poderia ser confidencial e/ou poderia incluir dados pessoais, de forma que o acesso ilegal a tais conteúdos poderia violar direitos que visam proteger a esfera pessoal do indivíduo, tais como o direito à privacidade, o direito ao sigilo da correspondência, o direito à proteção de dados etc. Em relação ao registro de outras informações relacionadas à original, ressalta-se que os dados adicionais podem representar violação a direitos da personalidade e, portanto, uma utilização ilegítima de tais dados pode infringir direitos no intuito de assegurar a sua proteção (CELESTE, 2019).

No que concerne à afetação do equilíbrio de poderes no ecossistema constitucional, Celeste (2019) afirma que as empresas privadas que produzem, vendem e gerenciam produtos e serviços de tecnologia digital no mundo estão a emergir no cenário constitucional como atores que atuam ao lado dos Estados-nação, assumindo uma posição igualmente dominante. Historicamente, o direito constitucional visava fornecer mecanismos de equilíbrio de poder, já que o Estado, por muito tempo, dominou o seio da política, sendo seu principal ator. Conseqüentemente, os instrumentos constitucionais criados o foram no intuito de limitar o seu poder, isto é, o poder estatal, visando garantir e proteger os direitos fundamentais individuais.

O problema é que a velocidade da tecnologia digital e a da teoria política são diferentes (a segunda não está conseguindo acompanhar o ritmo da primeira), pois o

Estado permanece com a tradicional obrigação de respeitar os direitos individuais, enquanto as entidades privadas não estão diretamente sujeitas a estas normas. Dessa forma, deve haver um reencontro de forças no cenário constitucional para assegurar que tais entidades também respeitem esses direitos, assim como deve haver a criação de novos mecanismos de limitação de poder que sejam mais adequados para lidar com tais – novas – relações. Afinal, na sociedade digital, é notório que as empresas tecnológicas também detêm uma forma de poder, qual seja o poder de regular o acesso e a utilização, pelos indivíduos, dos instrumentos de tecnologia digital e, conseqüentemente, afetar a forma como aqueles exercem os seus direitos através destes instrumentos (CELESTE, 2019).

Molinaro e Sarlet (2015) explicam que essa posição de destaque das empresas privadas se deu em decorrência do enfraquecimento gradual do papel do Estado no desenvolvimento de políticas econômicas de base, especialmente nos últimos anos, particularmente, a partir do acelerado processo de globalização, resultando em um quadro limitado de ação do Estado nacional na definição das políticas de Ciência e Tecnologia. Mendes e Fernandes (2020) apontam que iniciativas políticas e jurídicas voltadas à articulação de direitos, normas de governança e regras de limitação do poder na *internet* têm assumido centralidade como objetos de pesquisa do Direito Constitucional contemporâneo. No mesmo sentido, aduz Siqueira (2020) que, com o uso exponencial de dispositivos tecnológicos que dispõem de acesso à internet, mostra-se imprescindível a apreciação de sua influência no panorama constitucional dos direitos fundamentais.

Hoffmann-Riem (2020) relativiza a tese defendida por Celeste (2019) ao compreender que, no que tange à tarefa de adaptação do sistema jurídico, não haveria necessidade de estender os padrões jurídicos existentes para incluir as comunicações digitais ou de criar uma ordem especial para que os regramentos já conditos na Lei Fundamental possam ser utilizados a fim de evitar riscos associados à transformação digital. A verdade é que um direito estatal responsável e aplicável é indispensável como contrapeso ao crescente poder privado e para o devido controle pelo poder público nos amplos campos das aplicações das tecnologias de inteligência artificial. A Constituição Federal – CF de 1988 já deu um grande passo nesse sentido. Lima e Costa (2019, p. 174),

inclusive, explicam que a atual Carta Magna “foi a primeira a destinar um capítulo específico para a ciência e tecnologia e, com a Emenda Constitucional nº 85 de 2015, incluiu a inovação no referido capítulo, como um programa a ser implementado pelo Estado”³.

3 A PROTEÇÃO DOS DADOS PESSOAIS EM AMBIENTE VIRTUAL

Inicialmente, faz-se necessário apontar o conceito moderno de “dados pessoais” e Hoffmann-Riem (2020, p. 102) o faz de forma bastante objetiva, lecionando que “são considerados dados pessoais aqueles que se relacionam a uma pessoa natural identificada ou identificável”. Teixeira (2020, p. 50), ao seu turno, traz um conceito similar, no sentido de que “dado pessoal é uma informação relacionada a pessoa natural identificada ou identificável”. Percebe-se que, nos dois conceitos, a questão da identidade é crucial, na medida em que os dados não identificáveis ou tornados anônimos⁴ não podem ser enquadrados na categoria de dados pessoais.

Ademais, conforme explica Sarlet (2020, p. 193), os dados diferem das informações por serem “‘sinais’ ou ‘símbolos’ não interpretados, que, assim como os números, têm natureza formalizada, podendo ser reproduzidos e transmitidos mediante determinados procedimentos”. Dados são, pois, informações em potencial, existindo apenas em estado bruto, necessitando serem interpretados por quem os recebem, sendo desprovidos de sentido quando isoladamente considerados, ao contrário das informações.

Analisando um caso concreto julgado na Corte Superior alemã, Fritz e Mendes (2019) aduzem, do ponto de vista classificatório, que não existe motivação axiológica para tratar de forma diferenciada os dados digitais dos dados analógicos. Contudo, apesar dessa igualdade aparente, não se pode deixar de observar a relevância dos dados pessoais

³ Art. 218, CF/88: “O Estado promoverá e incentivará o desenvolvimento científico, a pesquisa e a capacitação tecnológicas” (BRASIL, 1988).

⁴ Hoffmann-Riem (2020, p. 102) aprofunda o debate e salienta “o impacto que a evolução das técnicas de desanonimização tem no conceito de dados pessoais, tendo em vista que um dado inicialmente anônimo – e, portanto, não enquadrado como dado pessoal – pode ser desanonimizável, possibilitando a sua devida identificação e enquadramento”.

digitais, especialmente em um contexto de massificação, produção, coleta, armazenamento, tratamento e compartilhamento desses dados no espaço virtual, tornando-os elementos relevantíssimos no sistema econômico mundial.

Mendes e Fonseca (2020) consignam que o direito à privacidade perpassou por transformações significativas, sobretudo em decorrência das mudanças tecnológicas que emergiram nas últimas décadas. Desse modo, os autores apontam que o sentido de privacidade evoluiu e passou a ser visto não só como uma liberdade negativa que serve de refúgio para o indivíduo (direito de ser deixado em paz), onde se confere proteção jurídica somente ao que é tido por íntimo ou privado, e não ao que é considerado público, mas também como uma liberdade positiva, consistente em um poder de exigir o conhecimento, o controle e a disposição de dados relativos à pessoa. Consequentemente, muitos começam a enxergar a garantia de proteção dos dados pessoais como algo que vai além do direito à privacidade: tem-se, a partir de então, um direito fundamental autônomo, cujo âmbito de proteção estaria relacionado ao cuidado da dignidade e da personalidade dos cidadãos no seio da sociedade da informação.

O tema privacidade não estava previsto na Constituição Federal de 1967 e o que motivou sua inclusão na atual Carta Magna⁵ foi a ampla devassa da vida privada e da intimidade, que acabava prejudicando a imagem das pessoas. Mesmo com a previsão constitucional, Teixeira (2020) indica que o Brasil passou um bom tempo sem uma posição clara a respeito da proteção jurídica à privacidade e de outros bens jurídicos diante da tecnologia da informação, mesmo com o desenvolvimento da *internet* e o seu alcance em território pátrio.

Por intermédio da Emenda Constitucional nº 115, de 2022, a CF de 1988 passou a prever, expressamente, o direito à proteção dos dados pessoais, inclusive nos meios digitais, como sendo um direito fundamental (art. 5º, inciso LXXIX). Antes mesmo da modificação no texto constitucional, algumas vozes doutrinárias, a exemplo de Sarlet

⁵ CF/88. Art. 5º, inciso X: são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).

(2020), já defendiam tal direito como sendo um direito fundamental implícito com fundamento no art. 5º, § 2º, do texto constitucional, sendo decorrência do sigilo das comunicações de dados (art. 5º, inciso II), da ação constitucional do *habeas data* (art. 5º, inciso LXXII), do princípio da dignidade da pessoa humana, do direito fundamental ao livre desenvolvimento da personalidade, do direito geral de liberdade e dos direitos à privacidade e intimidade:

Mas, possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana, que, de acordo com tradição jurídica já consolidada no direito constitucional estrangeiro e no direito internacional (universal e regional) dos direitos humanos, inclui o (mas não se limita ao!) direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa (SARLET, 2020, p. 185).

Apesar de já terem tramitado, no Congresso Nacional, inúmeros projetos para as questões jurídicas relacionadas à internet; somente em 23 de abril de 2014 foi promulgada a Lei nº 12.965, denominada Marco Civil da Internet (e apelidada de Constituição da Internet). Teixeira (2020) leciona que, com a promulgação dessa lei, o Brasil passou a ter uma posição mais clara a respeito da proteção jurídica da privacidade diante da internet, salientando-se que alguns dos seus pontos foram regulamentados pelo Decreto nº 8.771/2016⁶.

A verdade é que, no que tange ao tema, o Marco Civil da Internet pode ser compreendido como uma demarcação dos direitos do cidadão quanto ao uso da rede mundial de computadores no âmbito brasileiro, especialmente quanto à inviolabilidade da privacidade. Sobre o tema, a lei é clara, em seu art. 9, § 3º, ao dispor que “na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou

⁶ “Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações” (BRASIL, 2016).

roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados”.

Mendes e Fonseca (2020), ao abordar a permissão dada pelo usuário para compartilhamento de seus dados pessoais em sistemas virtuais, esclarece que os pressupostos que delineiam o paradigma do consentimento (a exemplo do Marco Civil da Internet) demonstram-se insuficientes para garantir um regime protetivo efetivo e material, especialmente para garantir um verdadeiro controle sobre o fluxo de dados pessoais pelo seu titular.

Os três pontos que elucidam as insuficiências do consentimento seriam: (i) as limitações cognitivas do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; (ii) as situações em que não há uma real liberdade de escolha do titular como, por exemplo, em circunstâncias denominadas de “*take it or leave it*”; e (iii) as modernas técnicas de tratamento e análise de dados a partir de *Big Data* que fazem com que a totalidade do valor e a possibilidade de uso desses dados não sejam completamente mensuráveis no momento em que o consentimento é requerido.

Sobre esse ponto, Teixeira (2020) aduz que o Marco Civil já trata de forma completa as questões que envolvem a captação de dados (normalmente via uso de *cookie*) e a formação de banco de dados (*mailing list*) e sua cessão ou comercialização para terceiros. No art. 7º da referida lei, o usuário tem direito: (i) a informações claras e completas sobre a coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que justifiquem sua coleta; e (ii) a necessidade de consentimento expresso sobre a coleta, uso, armazenamento e tratamento de dados pessoais deverá constar de forma destacada das demais cláusulas contratuais.

Além da captação, o art. 7º da “Constituição da Internet” prevê que é direito do usuário o não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei. Ressalta-se que a vedação do

fornecimento de dados é aplicável independente de a cessão a terceiro ser a título oneroso ou gratuito.

3.1 Lei Geral de Proteção de Dados Pessoais (LGPD), Transparência e Direitos do Titular

Os dados pessoais (especialmente os digitais) assumem, na sociedade contemporânea, importância estratégica cada vez maior. Podem ser utilizados em inúmeras aplicações, como o direcionamento de propagandas e anúncios específicos para o perfil de determinado consumidor, a partir das páginas que são visitadas na internet, ou a identificação da preferência ideológica ou mesmo sexual mediante análise dos gastos realizados pelo cartão de crédito, ou a investigação de doenças com maior probabilidade de se manifestarem durante a vida de determinado indivíduo, por meio da análise de seu material genético. Os exemplos são praticamente inesgotáveis e, cada vez mais, presentes no cotidiano – basta lembrar do smartphone, que sugere trajetos para o trabalho mesmo nos feriados (ROQUE, 2020).

Henrique (2022) explica que o problema nisso tudo é o enorme risco de utilização dos dados pessoais – muitas vezes colhidos sem o consentimento de seus titulares – para promover uma verdadeira devassa na vida privada. Além disso, não raras vezes esses dados são submetidos a tratamento por meio de algoritmos, a fim de realizar classificações, prognósticos ou mesmo julgamentos – que podem ser discriminatórios, ainda mais porque algoritmos frequentemente se baseiam em padrões passados, que podem ser o resultado de alguma distorção ou de injustiças da vida social

Diante desses riscos e considerando a preocupação crescente sobre o tema “proteção de dados pessoais”, a legislação brasileira deu um passo além do Marco Civil da Internet e incorporou ao ordenamento jurídico, em 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD). Inspirada em legislação europeia⁷, a lei aborda,

⁷ Em 2018, após grandes vazamentos de dados ocorrerem na União Europeia, viu-se a necessidade de criar novas regras de proteção de dados, a fim de regularizar o tratamento e a coleta destes, criando a *General*

especificamente, a questão do tratamento de dados, consistindo – de acordo com o seu art. 5º, inciso X – em toda operacionalização que diga respeito a dados pessoais, tais como “coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” de dados pessoais (BRASIL, 2018).

É importante explicitar que a LGPD alcança relações jurídicas estabelecidas digital e fisicamente, atingindo a todos que pratiquem tratamento de dados pessoais (agente controlador); podendo ser uma pessoa física ou uma pessoa jurídica (de direito público, como a União, Estados e Município e suas autarquias, ou de direito privado, como sociedades empresárias, associações, fundações, partidos políticos e igrejas), nos termos do art. 1º, *caput* c/c o art. 3º, *caput*.

Roque (2020, p. 16) aponta que são diversos os princípios que norteiam a LGPD, à exemplo da:

(a) boa-fé; (b) finalidade do tratamento; (c) compatibilidade do tratamento com as finalidades informadas ao titular; (d) limitação do tratamento ao mínimo necessário para a realização de suas finalidades; (e) garantia, aos titulares, de consulta facilitada e gratuita sobre a forma do tratamento; (f) garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; (g) transparência aos titulares; (h) utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais; e (i) prestação de contas, pelo agente, da adoção de medidas capazes de comprovar a proteção de dados pessoais.

Ainda, faz-se necessário apontar que o direito à privacidade, indicado por Roque (2020) como um dos princípios da LGPD, abrange o controle que o indivíduo tem sobre seus dados pessoais, de mantê-los indevidados as informações que digam a seu próprio respeito, assegurando-lhes controle sobre suas informações e a preservação de sua intimidade, protegendo-os da interferência ou vigilância de terceiros, seja o governo ou empresas privadas; ou seja, a vida privada, a liberdade de pensamento, crença ou opinião,

Data Protection Regulation (GDPR), que obrigou todas as empresas do mundo, em especial as famosas “Big Datas”, como Facebook e Google, a seguirem tais diretrizes (HENRIQUE, 2022).

necessitam de consentimento expresso para poderem ser compartilhadas por outro indivíduo (SILVA, 2023).

Nesse sentido é que o direito à privacidade vem ganhando novos contornos e significados, correspondendo ao direito reconhecido ao indivíduo de exercer o controle sobre o uso dos seus próprios dados pessoais inseridos num arquivo eletrônico (CARVALHO, PEDRINI, 2019).

O controle e a proteção dos dados na LGPD se dão, por exemplo, com a proibição de os provedores e *sites* utilizarem os dados dos usuários com finalidades comerciais, devendo manter essas informações sob sigilo pelo prazo mínimo de 6 (seis) meses; tratando-se de um comando que deverá ser cumprido, inclusive, por empresas estrangeiras que se submetam à legislação brasileira (BRASIL, 2018).

Carvalho e Pedrini (2019) esclarecem que a LGPD, no momento de sua promulgação, sofreu diversos vetos presidenciais que fragilizaram o sistema sancionatório da referida lei; isso porque, em comparação com a legislação europeia (GDPR); há, na LGPD, penas administrativas mais atenuadas, dentre as quais advertência, multa, publicização da infração, bloqueio dos dados pessoais; não havendo, contudo, a previsão de pena de suspensão das atividades de autoridades controladoras que violem os dados de um indivíduo.

No entanto, a proteção desses direitos poderá ser exercida em juízo (não só de forma individual, mas também coletivamente); é o que dispõe o art. 22 da referida lei. Além disso, o art. 42, caput, da LGPD faz menção ao fato de que a violação à legislação de proteção de dados pessoais pode acarretar danos patrimoniais ou morais, inclusive coletivos. Por fim, o § 3º do mesmo artigo estabelece que as ações de reparação por danos coletivos decorrentes da violação à proteção de dados pessoais podem ser exercidas coletivamente em juízo.

Percebe-se, desse modo, que há uma ampla gama de dispositivos legais com a finalidade de proteger os dados pessoais digitais de um indivíduo; contudo, com o surgimento de plataformas de realidade alternativa, a exemplo do Meta, faz-se oportuno

questionar: essas mesmas ferramentas seriam capazes de proteger os usuários numa rede de mundos virtuais?

4 META®: METAVERSO E REALIDADE VIRTUAL

Hoje, é muito comum que a vida social das pessoas se desenvolva não só física e presencialmente, mas também à distância, de forma virtual. Isso é plenamente perceptível em jovens e crianças, que utilizam seu tempo navegando pela *internet* desenvolvendo e praticando os mais diversos tipos de atividades. No entanto, Teixeira (2020) aponta que os mais velhos não estão imunes às tentações da Tecnologia da Informação, bastando reparar que, em uma roda de pessoas, ao invés de entabularem o diálogo presencial, valorizam o isolamento real para a inserção virtual.

Isso seria resultado, conforme apontam Lima e Costa (2019), de uma quarta revolução industrial, que seria caracterizada pela amplitude, profundidade e velocidade dos efeitos dos sistemas e máquinas inteligentes e conectados. Essa revolução, fruto da combinação de várias tecnologias, estaria desencadeando, na visão dos autores, mudanças na economia, na esfera pessoal, na cultura e nos próprios indivíduos – modificando “o que” as pessoas fazem e “como” elas agem.

Fortalece, então, uma nova espécie de meio ambiente, chamado de “meio ambiente virtual”. Teixeira (2020) conceitua esse espaço como sendo um local digital (não físico) em que as pessoas podem desenvolver os mais variados atos: se relacionar trocando mensagens, pesquisar, contratar, isto é, efetuar uma série de atitudes da vida social e econômica. No ambiente virtual, especialmente pelas mídias sociais, as pessoas estão encontrando novas formas de exercer a cidadania, manifestando-se e organizando-se.

Egliston e Carter (2021) descrevem a realidade virtual como um dispositivo de computação montado no corpo de uma pessoa (por exemplo, óculos de realidade virtual), criando experiências digitais ou simuladas por meio de áudio, *feedback* visual e tátil e permitindo uma sensação de presença fenomenológica ou de imersão no ambiente virtual.

Insera-se, nesse modelo, o *Meta*, que é uma realidade virtual criada pela empresa Facebook. Anunciado em 2021 pelo CEO da empresa, Mark Zuckerberg, o *Meta* representa um mundo virtual totalmente novo, aberto, compartilhável e tridimensional. Nesse universo, as pessoas poderiam criar avatares, novas identidades, novas personalidades e outras realidades sem as amarras da vida “real”⁸.

Já Cameron e Pearlman (2022) explicam o *Meta* como um mecanismo contextualizado no âmbito da realidade aumentada, da realidade virtual e da realidade mista – conhecidos coletivamente como realidade estendida. Tecnicamente, a realidade estendida presente no *Meta* permite uma fusão de todas as realidades simuladas mencionadas anteriormente, consistindo em experiências mediadas por tecnologia habilitadas por meio de um amplo espectro de *hardware* e *software*, incluindo interfaces sensoriais, aplicativos e infraestruturas. Todas essas ferramentas permitiriam um conteúdo de vídeo imersivo, experiências de mídia aprimoradas e experiências humanas interativas e multidimensionais, que permitirão o fluxo de indivíduos, dados, comércio e cultura em espaços 3D. Além disso, o metaverso permitirá, conforme defendem os autores, que os humanos criem, conectem, realizem comércio e até obtenham avaliação médica, diagnósticos, tratamento e terapia usando várias tecnologias convergentes.

Paulichi e Prux (2022, p. 25), por sua vez, definem esse projeto como “uma realidade digital, relacionada à *World Wide Web*, mas com elementos de redes sociais, realidade aumentada, games online e criptomoedas que permitem aos usuários agir e interagir virtualmente”. O fato é que a forma como o usuário irá se apresentar no metaverso irá criar uma espécie de “identidade digital” do sujeito, sendo, assim, uma projeção de sua identidade real, devendo ser protegida pelos direitos da personalidade,

⁸ “O metaverso teve seu embrião no jogo *Second Life*, criado em 2003 e que simulava uma vida em sociedade, por meio de avatares; porém, naquela ocasião, o jogo não tinha sequer conexão virtual, é dizer, o usuário não tinha interação entre o mundo real e o virtual. Após sua criação, o *Second Life* expandiu e ganhou em seu ambiente virtual novos negócios, como a disponibilização de imóveis virtuais e, inclusive, uma plataforma de marketplace, cuja moeda própria poderia ser utilizada no ambiente virtual do jogo. Tempos depois, o *Facebook* inovou, trazendo uma proposta de plena interação entre os mundos real e virtual, em que as pessoas pudessem se relacionar entre si, interagir e negociar com empresas, marcas, comprar propriedades virtuais, ou seja, criar seu próprio mundo virtual, em paralelo à ‘vida real’” (PIRONTI; KEPPEL, 2021, p. 58).

como direito a privacidade, intimidade, identidade e honra. Na percepção de Pironti e Keppen (2021), a LGPD considera, para fins de incidência das suas normas, o sujeito de direito como sendo a pessoa natural (art. 1º), de forma que os avatares devem ser considerados uma extensão da personalidade jurídica do seu titular, pois não é possível desvincular o criador da sua criatura, rompendo o nexu causal, quando a representação de um pelo outro se der de forma direta.

Em síntese, o avatar é uma extensão dos direitos de personalidade da pessoa natural que o criou, quando os dados coletados e tratados no metaverso representarem diretamente seu criador, afora essa hipótese, também é possível que seja o avatar considerado um dado pessoal de seu titular, caso ele próprio, avatar, seja utilizado na rede para identificar o seu criador. Em qualquer dos casos o Controlador de dados que realiza essa interface com os dados pessoais mantidos no mundo virtual deve agir sob a égide e os princípios da Lei Geral de Proteção de Dados. (PIRONTI; KEPPEEN, 2021, p. 64)

Apesar de parecer distante à realidade das pessoas, no âmbito jurídico já é possível observar a aplicação do metaverso: em setembro de 2022, foi realizada a primeira audiência judicial – na Justiça Federal na Paraíba –, em ambiente virtual imersivo e hiper-realista, utilizando-se de avatares em 3D, com o fim de realizar conciliação para pôr fim a um processo que tramitava desde 2018 (BRASIL, 2022).

Na mesma linha, a 2ª Vara de Família e Sucessões e o 2º Centro Judiciário de Soluções de Conflitos de Anápolis (MG) já está realizando atendimentos, reuniões, recebendo advogados e resolvendo questões administrativas em ambiente de realidade virtual aumentada. Em ambos os casos, o ingresso no metaverso se deu em decorrência da necessidade de adaptação do Poder Judiciário às novas tecnologias, bem como comunicação dos órgãos judiciais com um seguimento da sociedade ligado à tecnologia das informações (GOIÁS, 2022).

Percebe-se, desse modo, que as realidades virtuais possuem uma grande capacidade de impactar o comportamento dos seus usuários, principalmente dos adolescentes, por meio de jogos, das redes sociais e aplicativos. Com o metaverso, o modelo de negócios que está por trás dessa tecnologia é a obtenção de *superávit* de

pensamentos e sentimentos para ganhos alheios. Serva e Faria Junior (2022), nesse diapasão, apontam que a obtenção dos “comportamentos” humanos está para o modelo de negócios da *internet* como a obtenção dos “pensamentos e sentimentos” humanos está para o modelo de negócios do metaverso. E é aqui que surgem significativas preocupações com o que está por vir e quais os impactos da adoção desse modelo de negócios para os direitos humanos fundamentais.

Silva e Fernandes (2021) relatam que as obrigações assumidas no metaverso e os dados pessoais do avatar (e de seu criador) que circulam na rede, são protegidos pela LGPD, pois caracterizam dados da pessoa natural que deu “vida” ao avatar e, para isso, cadastrou tais dados na rede, como sua qualificação básica, suas senhas de acesso ou identificação facial ou digital, seu cartão de crédito ou outro meio de pagamento com “lastro real”.

Outro ponto interessante é a utilização de dispositivos tecnológicos, como os óculos de realidade virtual *Meta Quest*, que poderão ser utilizados como plataforma de acumulação de dados especiais. Nesse contexto, não se pode olvidar que o Meta tem como principal papel funcionar como uma plataforma de publicidade, gerando receita por meio da intermediação de transações entre anunciantes e usuários do referido software de realidade virtual. Desse modo, observa-se que a utilização desses equipamentos possibilitará uma maior captura de dados, permitindo o rastreamento e monitoramento da atividade dos usuários, e criando um vasto banco de dados que será utilizado para automatizar as trocas de dados entre anunciantes e o Meta - por meio de sua rede de anúncios (EGLISTON; CARTER, 2021).

Nesse sentido, Cameron e Pearlman (2022) refletem que, à medida que mais indivíduos e organizações passem a adotar o *Meta*, serão necessárias medidas de proteção específicas, haja vista que, nesse contexto de metaverso, o próprio conceito de privacidade precisará ser redefinido, ao considerar a superfície de ataque expandido. Além disso, as considerações tradicionais de proteção de dados precisarão ser relidas, levando em consideração o cérebro humano, a psicologia humana e os ambientes físicos circundantes.

Ao estudar os possíveis usos dos dados coletados pelas tecnologias do Meta, Kevins (2022) aponta que, a partir da abertura, fechamento, movimento e situação dos olhos, bem como a situação da pupila, as características da íris, os atributos faciais e a análise da marcha, haverá a possibilidade de minar dados concernentes aos traços da personalidade, saúde física e mental, habilidades pessoais, nível de sono, processo cognitivo, consumo de drogas, idade, identidade biométrica, histórico cultural, origem geográfica, gênero e carga de trabalho.

Muitos autores, como Martins, Fonseca e Lanfranqui (2022) se questionam se essa não seria a hora de parar e avaliar se os Estados não precisam colocar limites ao desenvolvimento dessas tecnologias, por mais encantadoras que sejam. Nesse sentido, aqui entra em destaque a concepção de constitucionalismo digital defendida por Mendes e Fernandes (2020), que não ignora a importância da jurisdição estatal na proteção dos direitos fundamentais.

Interessante é a solução proposta por Hoffmann-Riem (2020, p. 108), ao defender que uma maneira de “ampliar a proteção da autonomia dos usuários no futuro, seria obrigar os usuários (administradores) de dados [de terceiros] a fornecer aos usuários interfaces programáticas padronizadas para o acesso e gerenciamento de seus próprios dados pessoais”. Dessa forma, o usuário de uma plataforma digital poderia acompanhar, em tempo real, que dados pessoais seus foram coletados e como eles estão sendo utilizados e compartilhados.

No entanto, apesar da grande relevância dada à apresentação de informações pela entidade responsável pelo tratamento de dados, estudos indicados por Mendes e Fonseca (2020) têm indicado que, ao tomar decisões sobre sua privacidade e sobre seus dados, os indivíduos muitas vezes sequer leem regularmente as “Políticas de Privacidade” ou “Informações sobre o Uso de Dados” que lhe são apresentados, o que pode tornar a medida de fornecimento de ferramentas de controle ineficaz.

As cláusulas de adesão que definem as políticas de privacidade do Meta não são lidas, principalmente, em razão da complexidade do texto, que é pouco acessível para a maioria dos seus leitores. Nesse sentido, Miake (2022, p. 31) aduz que “alguns tópicos

são apenas subentendidos, deixando as especificidades da coleta ou da finalidade pouco claras; como é o caso dos ‘dados com proteções especiais’ que apenas indicam como o usuário pode optar por fornecer a informação ou não para outros perfis”.

Outro empecilho identificado por Miake (2022) nas Políticas de Privacidade é o fato de que frequentemente os textos apresentam *links* para informações mais específicas, mas não direciona para a informação a ser apresentada (*links* “quebrados”). Além disso, os links específicos de alguns produtos do Meta (Instagram, p. ex.) encontram-se em inglês. Esses são alguns dos fatores que dificultam o entendimento e a acessibilidade do leitor às informações contidas no documento, aspecto essencial para tornar a política de privacidade clara e de fácil acesso para todos os públicos.

No entanto, a Meta tem envidado esforços significativos nesse sentido, à exemplo de proposta de alteração do formato de divulgação da política de privacidade, que passará a conter textos mais curtos, divididos por tópicos, com mais exemplos e vídeos; para que os usuários entendam como as plataformas coletam, processam e compartilham as informações deles. O Vice-presidente de privacidade da Meta, Rob Sherman, confirmou que atualmente “a política de privacidade é uma grande muralha de texto; que, além de longa, é complicada para as pessoas entenderem” (MATHEWS, 2022, s/p). No entanto, para Rob Sherman, a nova proposta da empresa tentará deixar mais claros aspectos como (i) tipo de informação que a Meta coleta; (ii) como essas informações são usadas pelos aplicativos da empresa; e (iii) como a meta compartilha informações dos usuários com seus parceiros. Caso consolidado, tratar-se-á, portanto, de um grande avanço.

Nesse sentido, uma outra solução interessante seria aprimorar a ideia de consentimento quanto ao processamento de dados, considerando que, muitas vezes, os termos e condições gerais são unilateralmente elaborados pelas empresas e impostos aos usuários como verdadeiros “contratos de adesão”. Nesse sentido, uma maneira de amenizar essa situação seria a criação de uma espécie de certificação para as empresas através de organismos credenciados com reconhecimento público ou mesmo instituições oficiais especiais, a fim de verificar se os termos e condições gerais, por exemplo, cumprem os requisitos da legislação aplicável. Seria possível a previsão de represálias às

empresas que ou não atendessem às certificações, uma vez fiscalizadas, ou se negassem a passar por tais certificações. Ademais, seria interessante garantir, quando da inspeção, que tais termos e condições gerais não podem ser alterados sem a prévia comunicação aos interessados, bem como que tais termos são de fácil apreensão e compreensão pelos usuários, assegurando que o consentimento possa ser dado de forma autônoma e consciente por cada um deles (HOFFMANN-RIEM, 2020).

Outra medida recomendada por Hoffmann-Riem (2020, p. 114), com inspiração no direito norte-americano, seria a criação de uma agência federal especial, inspirada no poderoso *Federal Drug Administration*, especialmente para o pré-controle de algoritmos potencialmente perigosos.

No Brasil, a criação da Autoridade Nacional de Proteção de Dados (ANPD) parece contemplar a sugestão realizada por Hoffmann-Riem (2020), haja vista que a ANPD, além de fiscalizar, advertir e penalizar descumprimentos da Lei de Proteção de Dados, tem como função criar um elo entre a sociedade e o governo, permitindo que as pessoas encaminhem dúvidas, sugestões e denúncias ligadas à Lei de Proteção de Dados. Além disso, a ANPD desempenhará um importante papel pedagógico, pois agirá orientando e apoiando os órgãos do governo e as empresas em relação às situações em que elas poderão ou não tratar dados pessoais dos cidadãos (BRASIL, 2022).

Seja qual for a solução para o problema da coleta, uso e transferência de dados, Hoffmann-Riem (2020) defende que garantir a transparência suficiente é essencial não apenas para a proteção de dados, mas também para a proteção de outros interesses legalmente fundamentados. Nesse contexto, a transparência não deve ser um fim em si mesma, mas deve ser utilizável como base para a possibilidade de identificação de riscos e para a rastreabilidade e controlabilidade e, se necessário, para a possibilidade de revisão.

Essa medida se torna ainda mais necessária quando se observa a assimetria de poderes na relação entre o titular dos dados pessoais e os agentes responsáveis pelo tratamento desses dados, que repercute em uma discrepância no poder de barganha das partes, o que poderia prejudicar a tomada de uma decisão realmente livre e autônoma. Logo, faz-se necessário realizar uma consideração mais abrangente de como lidar com as

questões de segurança e privacidade no Meta, com o objetivo de desenvolver um pacote de soluções que permita os usuários escolherem e executarem as soluções que possam aliviar as preocupações relacionadas aos seus dados pessoais no metaverso.

5 CONSIDERAÇÕES FINAIS

Inicialmente, buscou-se compreender como surgiu o constitucionalismo digital. Verificou-se que, em sua criação, o direito constitucional visava fornecer mecanismos de equilíbrio de poder entre os atores estatais e garantir e proteger os direitos individuais das pessoas. Contudo, demonstrou-se, na primeira seção deste trabalho, que as empresas privadas têm se destacado no âmbito mundial, enfraquecendo de forma gradual o papel do Estado no desenvolvimento de políticas de ciência e tecnologia, surgindo, desse modo, o constitucionalismo digital, com o objetivo de defender a limitação do poder privado de atores da *internet*, em especial a proteção de direitos fundamentais no ciberespaço.

Em seguida, na segunda seção, estudou-se como se dá a proteção dos dados pessoais em um ambiente virtual. Primeiramente, apresentou-se o conceito de dados pessoais digitais, para depois abordar a garantia jurídica de proteção desses dados. Ressaltou-se a evolução que tem havido na garantia constitucional de direito à privacidade, em grande parte devido às mudanças tecnológicas que emergiram nas últimas décadas. Apontou-se, também, a legislação brasileira que circunda o tema, em especial, a Constituição Federal, o Marco Civil da Internet e a Lei Geral de Proteção de Dados.

Por fim, na última seção, buscou-se conceituar e explicar o funcionamento da tecnologia denominada metaverso, apontando, inclusive, algumas possibilidades de usos. Entretanto, o foco da seção foi sintetizar algumas das preocupações acerca dos impactos do sistema de realidade virtual “Meta” na proteção dos dados pessoais. Identificou-se que a utilização desse sistema possibilitará uma maior captura de dados, permitindo o rastreamento e monitoramento dos usuários, perfazendo um vasto banco de dados que poderá ser utilizado para automatizar o compartilhamento dos dados do usuário.

Conseqüentemente, percebeu-se que a ampliação do poder de comunicação das grandes empresas da internet impõe aos órgãos legislativos e judiciários a necessidade de definir um regime de responsabilidade civil dos intermediadores pelo conteúdo veiculado nessas redes. Contudo, a concepção, criação e implementação de regulamentos é difícil, tendo em vista a previsibilidade limitada do desenvolvimento futuro da digitalização e seus problemas subsequentes, mas, no final, é um desafio semelhante ao que tem sido e ainda é em outros campos do uso do Direito para influenciar os processos de inovação.

Também é provável que haja uma resistência considerável por parte de muitos, em especial daqueles desinteressados em medidas de regulamentação do uso de realidades virtuais e de outras tecnologias arriscadas, alegando, principalmente, se tratar de restrições desnecessárias à liberdade, dificultando a inovação tecnológica e social e aumentando a burocratização em contraposição à autoconfiguração.

Identificou-se, no desenvolvimento desta pesquisa, que os termos das políticas de privacidade do Meta são demasiadamente complexos e abstratos, impossibilitando uma compreensão mais transparente a respeito do concreto emprego dos dados. Contudo, foi possível localizar possíveis soluções para o problema, a exemplo do fornecimento aos usuários de interfaces programáticas padronizadas para o acesso e gerenciamento dos seus próprios dados pessoais.

Essa interface, na visão do presente trabalho, trará uma maior transparência acerca da captura e compartilhamento dos dados pessoais, na medida em que o usuário poderá ter conhecimento do tipo e quantidade de dados “colhidos” e de que forma e proporção suas informações estão sendo compartilhadas com terceiros.

Desse modo, entende-se que o objetivo geral e específicos foram devidamente atingidos, consciente de que modo algum almeja-se o esgotamento da temática. A pesquisa apresentada pretendeu meramente sugerir uma visão, a partir da avaliação do problema, não pretendendo ser uma resposta única ao tratamento constitucional do direito à privacidade, especialmente da proteção dos dados pessoais, no âmbito das tecnologias de realidade alternativa.

REFERÊNCIAS

BRASIL, Assembleia Constituinte. **Constituição Federal da República Federativa do Brasil de 1988**. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 set. 2022.

BRASIL, Ministério da Economia. **Quem vai regular a LGPD?** 2022. Disponível em: <https://www.serpro.gov.br/lgpd/governo/quem-vai-regular-e-fiscalizar-lgpd>. Acesso em: 24 set. 2022.

BRASIL, Presidência da República. **Decreto nº 8.771, de 11 de maio de 2016**. Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego (...). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 24 set. 2022.

BRASIL, Presidência da República. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 24 set. 2022.

BRASIL, Presidência da República. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 19 ago. 2023.

BRASIL. Justiça federal na Paraíba realiza primeira audiência real do Brasil no metaverso. **Justiça Federal**, 2022. Disponível em: <https://www.jfjb.jus.br/index.php/noticias/leitura-de-noticias?id=16221369>. Acesso em: 24 set. 2022.

CAMERON, Ryan; PEARLMAN, Kavya. Securing the metaverse – virtual worlds need real governance. **International Journal of Engineering Research and Technology**, v. 2, 2022. Disponível em: <https://bit.ly/3RmHuiW>. Acesso em: 24 set. 2022.

CARVALHO, Gisele Primo; PEDRINI, Tainá Fernanda. Direito à privacidade na lei geral de proteção de dados pessoais. **Revista da ESMESC**, v. 26, n. 32, 2019. Disponível em: <https://bit.ly/3E5wNgu>. Acesso em: 20 ago. 2023.

CELESTE, Edoardo. Digital constitutionalism: a new systematic theorisation. **International Review of Law, Computers & Technology**, v. 33, n. 1, p. 76-99, 2019. Disponível em: <https://bit.ly/3c8PiX0>. Acesso em: 17 ago. 2023.

EGLISTON, Ben; CARTER, Marcus. Critical questions for Facebook's virtual reality: data, power and the metaverse. **Internet Policy Review**, v. 10, i. 4, 2021. Disponível em: <https://eprints.qut.edu.au/230384/1/109122886.pdf>. Acesso em: 24 set. 2022.

FRITZ, Karina Nunes; MENDES, Laura Schertel. Case report: corte alemã reconhece a transmissibilidade da herança digital. **Revista Direito UNIFACS**, v. 15, n. 85, p. 188-211, 2019. Disponível em: <https://bit.ly/3ACwTeD>. Acesso em: 20 ago. 2022.

GOIÁS, Tribunal de Justiça do Estado. **Justiça goiana já está no Metaverso**. 2022. Disponível em: <https://www.tjgo.jus.br/index.php/institucional/centro-de-comunicacao-social/20-destaque/24953-justica-goiana-ja-esta-no-metaverso>. Acesso em: 24 set. 2022.

HENRIQUE, Gabriela Santoro. **Proteção de dados no metaverso**. Monografia (Graduação em Direito) – Universidade São Judas Tadeu. São Paulo, p. 26, 2022.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**. São Paulo: Forense, 2020.

KEVINS, Jerameel. Metaverse as a new emerging technology: an interrogation of opportunities and legal issues. **Columbia Law School, Public Law & Legal Theory Research Paper Series**. 2022. Disponível em: <https://dx.doi.org/10.2139/ssrn.4050898>. Acesso em: 24 set. 2022.

LIMA, Manuela Ithamar; COSTA, Sebastião P. Mendes da. Direito, inovação e ciência: possibilidades e desafios da sociedade do conhecimento. **Revista Arquivo Jurídico**, v. 6, n. 1, 2019. Disponível em: <https://bit.ly/3Dhz7Rz>. Acesso em: 19 ago. 2023.

MARTINS, Patrícia Helena Marta; FONSENCA, Victor Cabral; LANFRANQUI, Júlia Aragão. A evolução do metaverso na sociedade: principais desafios jurídicos. In: SEREC, Fernando Eduardo (Org.). **Metaverso: aspectos jurídicos**. São Paulo: Almedina, 2022.

MATHEWS, Eva. **Mudanças na política de privacidade da Apple e concorrência com TikTok pressionam Meta**. CNN Brasil, 2022. Disponível em: <https://bit.ly/3OAoo9C>. Acesso em: 20 ago. 2023.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. **Revista Brasileira de Direito**, v. 16, n. 1, 2020. Disponível em: <https://bit.ly/3cFpXV3>. Acesso em: 22 ago. 2023.

MENDES, Laura Schertel. FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista de Estudos Institucionais**, v. 6, n. 2, 2020. Disponível em: <https://bit.ly/3cFsPkF>. Acesso em: 15 ago. 2023

MIAKI, Caroline Medeiros. **Hackeando a privacidade: uma análise da política de dados do instagram**. Monografia (Graduação em Comunicação) – Universidade de Brasília. Distrito Federal, p. 43, 2022.

MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. Apontamentos sobre direito, ciência e tecnologia na perspectiva de políticas públicas sobre regulação em ciência e tecnologia. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia. (Coord.). **Direito, inovação e tecnologia**, v. 1. São Paulo: Saraiva, 2015.

PAULICHI, Jaqueline Silva; PRUX, Oscar Ivan. A realidade simulada do metaverso, San Junipero e os direitos da personalidade. **Revista de Sociologia, Antropologia e Cultura Jurídica**, v. 8, n. 1, 2022. Disponível em: <https://bit.ly/3Bdph2y>. Acesso em: 10 ago. 2022.

PIRONTI, Rodrigo; KEPPEN, Mariana. Metaverso: novos horizontes, novos desafios. **International Journal of Digital Law**, Belo Horizonte, ano 2, n. 3, p. 57-67, set./dez. 2021. DOI: 10.47975/IJDL.pironti.v.2.n.3.

ROQUE, André. A tutela coletiva dos dados pessoais na lei geral de proteção de dados pessoais (LGPD). **Revista Eletrônica de Direito Processual**, ano 13, v. 20, n. 2, 2019. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/redp/article/view/42138/30270>. Acesso em: 19 ago. 2023.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988. **Revista Brasileira de Direitos Fundamentais e Justiça** v. 14, n. 42, 2020. Disponível em: <https://dfj.emnuvens.com.br/dfj/article/view/875>. Acesso em: 01 ago. 2023.

SERVA, Clara; FARIA JUNIOR, Luiz Carlos Silva. Direitos humanos no metaverso: direitos reais de pessoas virtuais. *In*: SEREC, Fernando Eduardo (Org.). **Metaverso: aspectos jurídicos**. São Paulo: Almedina, 2022.

SILVA, Danilo Morais da; FERNANDES, Valdir. Ciberespaço, cibercultura e metaverso: a sociedade virtual e território cibernético. **Revista Humanidades e Inovação**, v. 8, n. 67, 2021. Disponível em: <https://bit.ly/3ReLWB3>. Acesso em: 18 ago. 2023.

SILVA, Sâmelá Cesar da Silva. **A lei de proteção de dados sob o advento do metaverso**. Monografia (Graduação em Direito) – Escola de Ciências Jurídicas da Universidade Anhembi Morumbi. São Paulo, p. 62, 2023.

SIQUEIRA, Andressa de Bittencourt Siqueira. A fundamentalidade subordinada do direito de acesso à internet no cenário jurídico-constitucional brasileiro. **Revista Eletrônica de Direito Público**, v. 7, 2020. Disponível em: <https://bit.ly/3JbCT2N>. Acesso em: 19 ago. 2023.

TEIXEIRA, Tarcísio. **Direito digital e processo eletrônico**. 5ª ed. São Paulo: Editora Saraiva, 2020.