UNIVERSIDADE FEDERAL DO CEARÁ

CAMPUS DE QUIXADÁ

CURSO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

VITOR WILLIAN CORREIA DE OLIVEIRA

CONFORMIDADE DO METAVERSO DA EMPRESA META COM A LGPD: ANÁLISE DAS PRÁTICAS DE COLETA, TRATAMENTO E PROTEÇÃO DE DADOS

QUIXADÁ

2024

VITOR WILLIAN CORREIA DE OLIVEIRA

CONFORMIDADE DO METAVERSO DA EMPRESA META COM A LGPD: ANÁLISE DAS PRÁTICAS DE COLETA, TRATAMENTO E PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Roberto Cabral Rabelo Filho

QUIXADÁ

2024

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Sistema de Bibliotecas
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

O52c Oliveira, Vitor Willian Correia de.
Conformidade do metaverso da empresa meta com a lgpd: análise das práticas de coleta, tratamento e proteção de dados. / Vitor Willian Correia de Oliveira. – 2024.
54 f. : il.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Sistemas de Informação, Quixadá, 2024.
Orientação: Prof. Dr. Roberto Cabral Rabêlo Filho.

1. Metaverso. 2. LGPD. 3. Dados Sensíveis. 4. Coleta de Dados. 5. Tratamento dos Dados. I. Título.
CDD 005

VITOR WILLIAN CORREIA DE OLIVEIRA

CONFORMIDADE DO METAVERSO DA EMPRESA META COM A LGPD: ANÁLISE DAS PRÁTICAS DE COLETA, TRATAMENTO E PROTEÇÃO DE DADOS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Sistemas de Informação do Campus de Quixadá da Universidade Federal do Ceará, como requisito parcial à obtenção do grau de bacharel em Sistemas de Informação.

Aprovada em: 01/10/2024

BANCA EXAMINADORA

Prof. Dr. Roberto Cabral Rabelo Filho (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Antônio Joel Ramiro de Castro
Universidade Federal do Ceará (UFC)

Prof. Dr. Sidartha Azevedo Lobo de Carvalho
Universidade Federal do Ceará (UFC)

AGRADECIMENTOS

A Deus agradeço por guiar sempre meus passos nos momentos de dificuldade enfrentados neste meu percurso pela faculdade.

Agradeço ao meu orientador Roberto Cabral, cujo apoio contínuo, orientação e críticas construtivas foram fundamentais para o desenvolvimento desta pesquisa.

Aos colegas e amigos, que ofereceram suporte moral e incentivo ao longo do processo, meu profundo agradecimento. Suas palavras de encorajamento e ajuda prática foram indispensáveis.

Agradeço à minha família pelo amor, paciência e compreensão durante a realização deste trabalho. Seu apoio incondicional foi um pilar fundamental para a conclusão desta pesquisa.

A todos, meu mais sincero agradecimento.

RESUMO

Com o avanço das tecnologias digitais e a crescente adoção de ambientes virtuais, como o Metaverso desenvolvido pela empresa Meta, a proteção de dados pessoais emergiu como uma questão crucial. O presente estudo tem como objetivo investigar a conformidade do Metaverso da empresa Meta com a Lei Geral de Proteção de Dados (LGPD), focalizando as práticas relativas à coleta, tratamento e proteção de dados pessoais. A pesquisa consiste em uma análise detalhada das práticas implementadas pela Meta e uma comparação com os princípios estabelecidos pela LGPD para verificar sua conformidade. A análise das práticas de coleta de dados do Horizon Worlds revelou que a Meta está em conformidade com a maioria dos princípios da LGPD. O consentimento do titular é obtido no momento da criação da conta, garantindo que os usuários estejam informados sobre o uso de seus dados, incluindo sensores como microfone e rastreamento ocular. Além disso, em conformidade com obrigações legais, a Meta solicita informações como a data de nascimento para proteger usuários menores de idade, de acordo com as leis de proteção infantil. No entanto, algumas áreas não se aplicam diretamente ao Horizon Worlds, como a administração pública e a proteção de crédito. Para esses casos, o estudo sugere melhorias, como a criação de uma equipe especializada em regulamentações locais e a implementação de sistemas mais robustos para proteger dados financeiros durante transações. Por fim, a Meta assegura que os dados dos usuários são processados de maneira segura e transparente, com mecanismos de eliminação de dados quando necessário, cumprindo as obrigações estabelecidas pela LGPD. A pesquisa conclui com melhorias para abordar lacunas e enfatiza a necessidade de uma revisão contínua das práticas de segurança e proteção de dados.

Palavras-chave: metaverso; LGPD; proteção de dados; coleta de dados; tratamento de dados; segurança da informação.

ABSTRACT

With the advancement of digital technologies and the growing adoption of virtual environments, such as the Metaverse developed by Meta, the protection of personal data has emerged as a crucial issue. This study aims to investigate the compliance of Meta's Metaverse with the General Data Protection Law (LGPD), focusing on practices related to the collection, processing, and protection of personal data. The research consists of a detailed analysis of the practices implemented by Meta and a comparison with the principles established by the LGPD to verify its compliance. The analysis of Horizon Worlds' data collection practices revealed that Meta complies with most of the LGPD principles. User consent is obtained at the time of account creation, ensuring that users are informed about how their data, including sensors such as microphones and eye tracking, will be used. Additionally, in compliance with legal obligations, Meta requests information such as the date of birth to protect underage users, in accordance with child protection laws. However, some areas do not apply directly to Horizon Worlds, such as public administration and credit protection. For these cases, the study suggests improvements, such as the creation of a specialized team in local regulations and the implementation of more robust systems to protect financial data during transactions. Lastly, Meta ensures that users' data is processed securely and transparently, with data deletion mechanisms in place when necessary, fulfilling the obligations established by the LGPD. The study concludes with suggestions for improvements to address gaps and emphasizes the need for ongoing review of security and data protection practices.

Keywords: metaverse; LGPD; data protection; data collection; data processing; information security.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANPD	Autoridade Nacional de Proteção de Dados Pessoais
AR	*Augmented Reality*
CCPA	Lei de Privacidade do Consumidor da Califórnia
CCVE	Código de Conduta para Experiências Virtuais
GDPR	Regulamento Geral sobre a Proteção de Dados
HMDs	Head-mounted displays
LAI	Lei de Acesso à Informação
LGPD	Lei Geral de Proteção de Dados
MEMS	microeletromecânicos
NFTs	*Non-fungible Tokens*
Serpro	Serviço Federal de Processamento de Dados
VR	*Virtual Reality*

SUMÁRIO

1 INTRODUÇÃO

No atual contexto de desenvolvimento de ambientes virtuais, a proposta do Metaverso está próxima de ser concretizada e também é amplamente esperada como a próxima evolução da Internet (Cheng, R. *et al.*, 2022). Grandes empresas como Meta, Microsoft, Roblox e outras gigantes da tecnologia estão investindo pesado nesse projeto que visa criar um ambiente virtual compartilhado, onde as pessoas possam se encontrar, trabalhar, se divertir e consumir determinados serviços (Tecnoblog, 2021).

Sendo assim, espera-se que o convívio social das pessoas esteja cada vez mais próximo de uma digitalização completa e, por esse motivo, espera-se que problemas relacionados a segurança de informação cresçam conforme esse projeto avança. No entanto, a implementação do metaverso enfrenta alguns desafios técnicos e culturais (CodeCrush, 2022). Um dos principais desafios é garantir a segurança e privacidade dos usuários, especialmente quando se trata de compartilhar informações sensíveis em um ambiente virtual. Neste cenário, a privacidade e a proteção dos dados se tornaram fatores fundamentais para que a tecnologia continue a se desenvolver de maneira sustentável e correta (Ferreira, L. *et al.*, 2022).

O termo "Metaverso" foi utilizado pela primeira vez em um romance de ficção científica chamado *"Snow Crash"* escrito em 1992 por Neil Stephenson (Joshua, 2017). Nesse livro o metaverso é descrito como um mundo paralelo ao que vivemos, onde as pessoas, por meio de dispositivos de realidade virtual, imergem nesse mundo e interagem nesse ambiente juntamente com outras pessoas através de seus avatares. Eles seriam suas representações virtuais, mas para que este ambiente virtual compartilhado consiga ser implementado existem grandes desafios que precisam ser enfrentados por seus idealizadores, e nesta pesquisa trataremos de um desses desafios.

Em um ambiente virtual compartilhado, as informações dos usuários podem ser facilmente expostas a hackers, cibercriminosos e outros usuários mal-intencionados (Fia, 2023). Conforme a norma Associação Brasileira de Normas Técnicas (ABNT) NBR ISO/IEC 27002, a Segurança da Informação é caracterizada pela preservação da disponibilidade, integridade e confidencialidade da informação, além de outras propriedades como Autenticidade, Confiabilidade, Não-Repúdio e Responsabilidade sobre a informação.

Uma falha de segurança é definida por qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de

tratamento de dados inadequada ou ilícita(UFRJ, 2023).

No decorrer deste trabalho veremos que questões como percepções de privacidade e normas da Lei Geral de Proteção de Dados (LGPD), em relação à coleta e proteção de dados, desempenham um papel crucial na segurança da informação para o Metaverso.

A LGPD é a legislação do Brasil que controla o tratamento de dados pessoais, definindo diretrizes para a coleta, armazenamento, utilização, compartilhamento e exclusão de dados pessoais no país. Criada em 2018, a LGPD visa proteger a privacidade e os direitos essenciais dos cidadãos, assegurando um maior domínio sobre seus dados pessoais.

Dentro do Metaverso, a LGPD é indispensável, já que ele trata de um grande volume de dados sensíveis dos usuários. É fundamental que as empresas, como a Meta, que atuam no Metaverso, sigam as diretrizes da LGPD para assegurar a proteção dos dados pessoais, evitando violações e uso indevido das informações. Pois as informações pessoais são frequentemente alvo de ataques cibernéticos e violações de dados (Lobo, 2023).

Sendo assim, chega-se ao seguinte questionamento: o Metaverso da empresa Meta está adéquo leis nacionais de segurança da informação para que seus usuários não tenham seus dados pessoais acessados de maneira indevida?

Para responder essa pergunta, esta pesquisa investiga se o Metaverso da empresa Meta apresenta inadequações em relação às exigências da LGPD brasileira e os métodos empregados para evitar o acesso inadequado de dados pessoais.

1.1 OBJETIVOS

1.1.1 Geral

Identificar a adequação do Metaverso desenvolvido pela empresa Meta com as normas de segurança de dados da LGPD.

1.1.2 Específicos

1. Elencar uma análise detalhada das práticas de segurança do Metaverso da empresa Meta em relação à proteção de dados sensíveis.
2. Analisar as práticas de coleta, armazenamento, processamento e compartilhamento de dados pessoais no Metaverso da empresa Meta.
3. Denotar as orientações de coleta, armazenamento, processamento e compartilhamento de

dados pessoais da LGPD.

4. Apontar as inconformidades do Metaverso da empresa Meta com a LGPD sobre coleta, armazenamento, processamento e compartilhamento de dados.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção, serão explorados os fundamentos teóricos por trás das regulamentações da LGPD, seus principais controles de segurança da informação, os direitos e princípios estabelecidos por ela e uma apresentação da proposta do Metaverso com seus desafios.

2.1 METAVERSO

Esta subseção apresentará uma breve descrição sobre o que é o Metaverso, suas camadas e como a segurança é feita nesse ambiente.

2.1.1 Descrição

O termo "Metaverso" foi utilizado pela primeira vez em um romance de ficção científica chamado *"Snow Crash"* escrito em 1992 por Neil Stephenson (Joshua, 2017). O romance se passa num mundo cibernético paralelo ao mundo real, chamado exatamente de Metaverso, no qual as pessoas reais possuem um avatar digital. Neste ambiente eles interagem e vivem uns com os outros por meio dos avatares.

De acordo com *newzoo* (Newzoo, 2021), sustenta-se que ainda não existe uma definição única, ou oficial, mas que muita gente ensaia definições para o metaverso. Entretanto, pode-se citar que uma dessas definições é: o Metaverso é o conjunto de mundos virtuais coletivos, online, persistentes e em 3D onde todo o conteúdo é criado pelos usuários, é um espaço virtual onde os usuários podem criar, explorar e se encontrar sem precisar estar no mesmo espaço real (Eno, J. *et al.*, 2009).

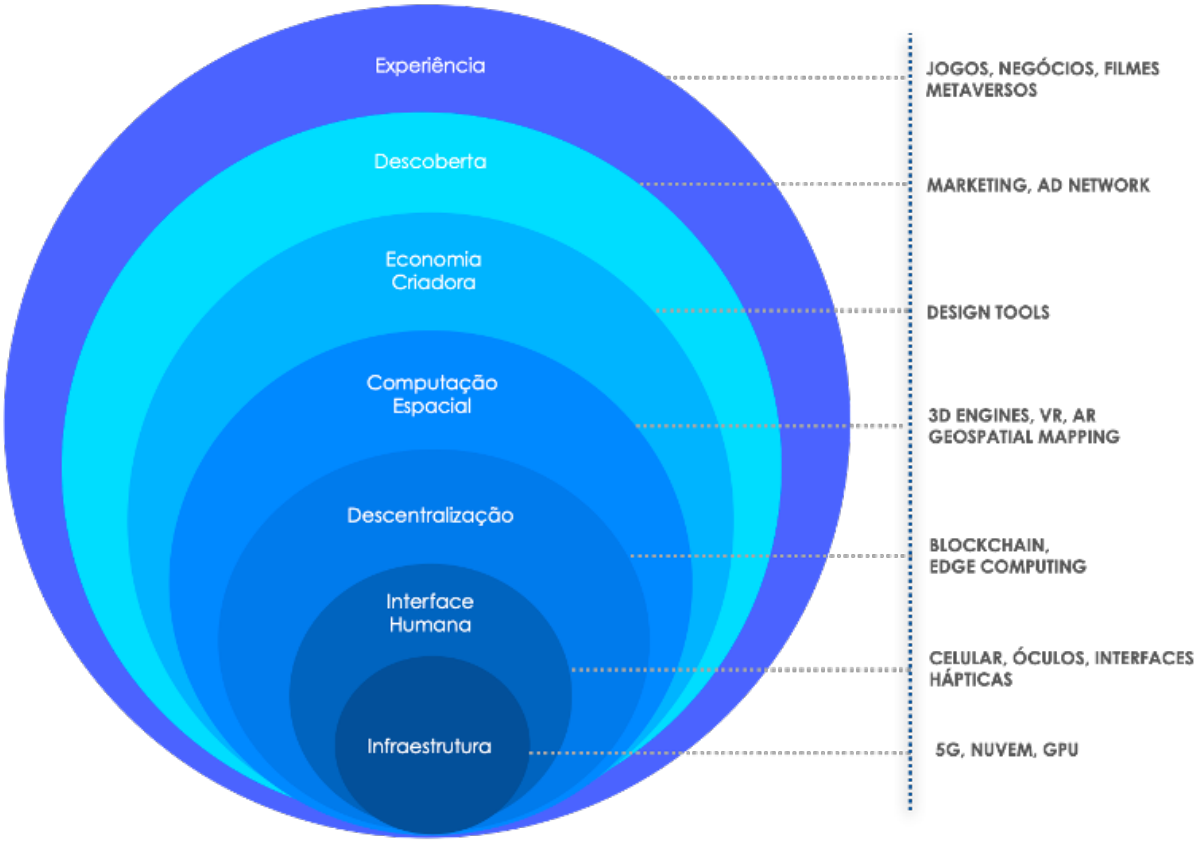
O Metaverso é sem dúvida muito complexo em estrutura, Jon Radoff, um empreendedor, autor e designer de jogos, publicou na plataforma *Medium* a sua concepção detalhada sobre as sete camadas do Metaverso (Radoff, 2021), em seu artigo, Radoff fornece uma descrição da cadeia de valor do Metaverso, desde as experiências que as pessoas buscam até as tecnologias habilitadoras que tornam isso possível. Vejamos agora uma breve descrição dessas camadas.

2.1.2 Camadas do Metaverso

Radoff em seu artigo define as 7 camadas do Metaverso como, experiência, descoberta, economia dos criadores, computação espacial, descentralização, interface humana e

infraestrutura, veja a Figura 1.

Figura 1 – Camadas do Metaverso



Fonte: Adaptado de Radoff (2021)

As camadas Experiência, Descoberta e Economia dos Criadores formam a parte de produtos, aplicativos e ecossistemas operacionais. As camadas de Computação Espacial e Descentralização correspondem às ferramentas de desenvolvimento. Interface Humana e Infraestrutura referem-se as tecnologias e a própria infraestrutura necessária ao metaverso.

Vejamos as definições das camadas segundo Radoff em seu artigo: *The Metaverse Value-Chain*, 2021.

1. Experiência:

   Segundo Radoff essa camada está ligada à experiência do usuário dentro do Metaverso, incluindo jogos, interação social, compras e muitas outras atividades.

2. Descoberta:

   De acordo com Radoff: “Uma forma específica de destaque da comunidade é a presença em tempo real. Isso é extremamente relevante em um metaverso, aonde grande parte do valor surgirá da interação com amigos por meio de experiências compartilhadas.”. Isso significa que a descoberta em grupo será um dos fatores importantíssimos do Metaverso.

Assim, essa camada representa as atrações que introduzem os seres humanos a novas experiências.

3. Economia dos criadores:

   Até agora, as experiências impulsionadas por criadores no metaverso estão centradas em plataformas gerenciadas centralmente, como Roblox, Rec Room e Manticore. Essa é a camada que contém toda a tecnologia que os criadores usam diariamente para criar as experiências que as pessoas desfrutam.

4. Computação espacial:

   Computação espacial é a interação humana com uma máquina na qual a máquina mantém e manipula referências a objetos e espaços reais (Greenwold, 1995). E no metaverso ela representa as tecnologias utilizadas para criar e interagir com o ambiente.

5. Descentralização:

   Essa camada, possivelmente, é a mais estratégica do Metaverso, pois ela traz a liberdade para todas as pessoas. Isso implica que o metaverso não será controlado por nenhuma instituição ou empresa. E é importante ressaltar que o Blockchain, as *Non-fungible Tokens* (NFTs) e a inteligência artificial estarão presentes nessa camada.

6. Interface humana:

   Nessa camada estarão presentes os conceitos de *Augmented Reality* (AR) e *Virtual Reality* (VR), a camada dependerá muito da evolução de equipamentos capazes de unir o "humano" e a "máquina", para proporcionar novas maneiras de interagir com a tecnologia além do computador e do smartphone.

7. Infraestrutura:

   Essa camada é a base técnica para todo o Metaverso, nela está a tecnologia que permite nossos dispositivos conectarem-se à rede e entregarem conteúdos. Para essa finalidade será fundamental, além de hardwares diminutos e poderosos, as redes 5G e 6G, pois elas melhorarão drasticamente a largura de banda, reduzindo a contenção de rede e a latência. De acordo com Radoff, essa tecnologia exigirá semicondutores prestes a atingir processos de 3nm e além, e também sistemas microeletromecânicos (MEMS) que facilitam sensores pequenos e baterias compactas de longa duração.

A governança de mundos virtuais massivos como esse apresenta desafios para regular o comportamento dos usuários. Portanto, o metaverso requer regulamentações e políticas para gerenciar a plataforma e seus membros (Fernandez; Hui, 2022).

Não existe uma camada específica que esteja diretamente ligada a segurança, privacidade e governança no Metaverso. Esses aspectos são considerados requisitos transversais que permeiam todas as camadas do metaverso (Vadlamudi, 2022). Vejamos agora medidas utilizadas pelo Metaverso para abranger esses aspectos.

2.1.3 Privacidade e Segurança no Metaverso

O Metaverso utiliza dados coletados do mundo real para criar experiências imersivas. Por meio de sensores acoplados aos usuários, como giroscópios para rastrear os movimentos da cabeça, é possível controlar realisticamente avatares. No entanto, o Metaverso também enfrenta alguns desafios, especialmente em relação à privacidade dos usuários. Em seus vastos mundos virtuais, os usuários podem se tornar alvos de ataques, como a espionagem por parte de outros usuários da plataforma (Fernandez; Hui, 2022).

Outro exemplo que podemos citar são os sensores comumente usados para exibir o metaverso. Esses sensores normalmente são os Head-mounted displays (HMDs), um tipo de display com uma forma de “capacete”, que possui dois visores que controlam a direção em que o usuário está olhando para atualizar as imagens do mundo virtual, eles podem coletar alguns dados biométricos que não são óbvios para os usuários. Como os dados de rastreamento ocular que podem revelar as preferências sexuais dos usuários (Roesner, F. *et al.*, 2014).

Por motivos como esse, os dados devem ser tratados de acordo com alguns princípios que protejam a privacidade dos usuários, e nesse âmbito entram as diretrizes de proteção de dados da LGPD.

2.2 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Esta seção apresentará conceitos da LGPD e informações importantes como sua origem e finalidade.

2.2.1 Descrição

Aprovada em agosto de 2018, a Lei n° 13.709, está em vigência desde agosto de 2020, promulgada para proteger os direitos fundamentais de liberdade, privacidade e da livre formação da personalidade de cada indivíduo (Brasil, 2018). A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito

público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.

Essa lei estabelece uma padronização da maneira que as informações devem ser armazenadas, informações essas que, como dito previamente, podem ser tanto no meio físico como digital, e segundo a mesma, a finalidade e a necessidade do uso dos dados precisam estar claras para os cidadãos. Caso ocorra um vazamento de dados deve-se seguir um protocolo onde a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e os envolvidos devem ser notificados, e vale ressaltar que tais falhas podem resultar em multas e penalidades.

Oficialmente a Lei n° 13.709/2018 está dividida em 10 capítulos com 65 artigos ao total.

1. CAPÍTULO I - DISPOSIÇÕES PRELIMINARES
2. CAPÍTULO II - DO TRATAMENTO DE DADOS PESSOAIS
3. CAPÍTULO III - DOS DIREITOS DO TITULAR
4. CAPÍTULO IV - DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO
5. CAPÍTULO V - DA TRANSFERÊNCIA INTERNACIONAL DE DADOS
6. CAPÍTULO VI - DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS
7. CAPÍTULO VII - DA SEGURANÇA E DAS BOAS PRÁTICAS
8. CAPÍTULO VIII - DA FISCALIZAÇÃO
9. CAPÍTULO IX - DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD) E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE
10. CAPÍTULO X - DISPOSIÇÕES FINAIS E TRANSITÓRIAS

O estudo da LGPD que será mostrado neste trabalho usa como principal fonte o documento “LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) - Guia de Boas Práticas para Implementação na Administração Pública Federal” (Brasil, 2020), e nesse trabalho em específico serão abordados principalmente os capítulos II, III, IV e VII descritos anteriormente.

A adequação de órgãos públicos e privados à LGPD é relacionada a uma mudança cultural da empresa em todos os seus três níveis de planejamento, isto é, nível estratégico, tático e operacional. Essa mudança de cultura implica em considerar a privacidade dos dados dos cidadãos desde a coleta até a sua execução (Privacidade by Desing).

Essa Lei possui um princípio muito importante onde o propósito do tratamento de dados seja: “legítimo, específico, explícito e informado ao titular”, isso significa que todo o

processo em que os dados de uma pessoa possam ser utilizados na organização seja de pleno conhecimento desse indivíduo. E as demais orientações sobre o tratamento de dados descritas no documento que serve de base para esse trabalho, podem ser resumidas em 4 tópicos: direitos fundamentais do proprietário dos dados, tratamento dos dados pessoais, ciclo de vida dos dados e boas práticas em Segurança da Informação.

2.2.2 Direitos fundamentais do proprietário dos dados

Inicialmente alguns conceitos essenciais devem ser descritos para a compreensão dos direitos do proprietário dos dados. São eles o Controlador, Operador, Encarregado e "tratamento de dados".

Segundo o Art. 5º da LGPD, o tratamento de dados pessoais pode ser realizado por duas entidades chamadas "agentes de tratamento", nomeados por Controlador e o outro de Operador. Tratamento definido na seção X da Lei como: "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

Conforme a seção VI da LGPD do mesmo artigo, o Controlador é definido como pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Isto refere-se à entidade que será atribuída a função de adotar decisões sobre o tratamento de dados.

Na seção VII o Operador é descrito por: "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.", nesta descrição estão inclusos aqueles que exercem a atividade de tratamento no âmbito de contrato ou instrumento similar.

Além dos Agentes de tratamento existe uma figura descrita na seção VIII chamada de "Encarregado", que exerce uma função muito importante no cumprimento da LGPD, e sua função é de agir como um canal de comunicação entre o titular dos dados (pessoa natural a quem se referem os dados pessoais que são objeto de tratamento), o controlador e a ANPD.

Visto esses conceitos, o Quadro 1 descreve os direitos garantidos pela LGPD aos titulares de dados conforme o art. 6° da Lei:

Quadro 1 – Direitos garantidos aos titulares de dados

DIREITOS DOS TITULARES	PRINCÍPIO CORRESPONDENTE	REFERÊNCIA LEGISLATIVA (LGPD)
Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades	Princípio da finalidade	Art. 6º, I
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Princípio da adequação	Art. 6º, II
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Princípio da necessidade	Art. 6°,III
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais	Princípio do livre acesso	Art. 6º, IV
Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento	Princípio da qualidade dos dados	Art. 6º, V
Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial	Princípio da transparência	Art. 6º, VI
Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão	Princípio da segurança	Art. 6º, VII
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais	Princípio da prevenção	Art. 6º, VIII
Direito de não ser discriminado de forma ilícita ou abusiva	Princípio da não discriminação	Art. 6º, IX
Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais	Princípio da responsabilização e prestação de contas	Art. 6º, X

Fonte: Adaptado de Brasil (2020)

2.2.3 Tratamento dos dados pessoais

Nesse tópico veremos como os dados dos titulares devem ser tratados segundo a LGPD, e segundo o Art. 5º da lei, devemos ter conhecimento prévio de qual tipo de dado estará em tratamento, podendo ser:

1. Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
2. Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa,

opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

3. Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Além desses conhecimentos vale ressaltar que a autorização sobre o tratamento de dados sensíveis só é disponível em situações indispensáveis assim como consta no art. 7º, I.

Ao se observar no art. 6° vemos os princípios referentes ao tratamento de dados assim como consta no Quadro 1, mas esses dados possuem um ciclo de vida que veremos na próxima subseção.

2.2.4 Ciclo de vida dos dados

Assim como foi apresentado na subseção anterior, a LGPD considera como tratamento toda operação realizada com os dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Assim o ciclo de vida do tratamento tem início com a coleta do dado e se encerra com a eliminação ou descarte (SEF, 2020), veja a Figura 2.

Figura 2 – Ciclo de vida dos dados pessoais - LGPD

Fonte: Adaptado de SEF (2020)

O Quadro 2 descreve as fases de tratamento da Figura 2 com sua relação com as operações da LGPD descritas no art. 5° da lei.

Vale ressaltar que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado, ou ilícito, assim como consta no art. 46°, VII.

Quadro 2 – Descrição das fases do ciclo de vida e operações dos dados pessoais.

Fase do ciclo	Descrição	Operações de tratamento - LGPD, ART. 5º, X.
Coleta	Obtenção, recepção ou produção de dados pessoais independente do meio utilizado(documento em papel, documento eletrônico, sistema de informação, etc.)	Coleta, produção, recepção.
Retenção	Arquivamento ou armazenamento de dados pessoais independente do meio utilizado (documento em papel, documento eletrônico, banco de dados, arquivo de aço, etc.).	Arquivamento e armazenamento.
Processamento	Qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação.
Compartilhamento	Qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais	Transmissão, distribuição, comunicação, transferência e difusão.
Eliminação	Qualquer operação que visa apagar ou eliminar dados pessoais. Esta fase também contempla descarte dos ativos organizacionais nos casos necessários ao negócio da instituição.	Eliminação.

Fonte: Elaborado pelo autor

2.2.5 Penalidades para Violações

No caso de descumprimento das regras estabelecidas na LGPD, a ANPD pode impor sanções administrativas conforme o Artigo 52 da lei.

1. Advertência:

   Com prazo para adoção de medidas corretivas.

2. Multa Simples:

   Até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, no seu último exercício, excluídos os tributos, limitada a R$ 50.000.000,00 por infração.

3. Multa Diária:

   Observado o limite total mencionado na multa simples.

4. Publicização da Infração:

   Após devidamente apurada e confirmada a sua ocorrência.

5. Bloqueio dos Dados Pessoais:

   Relativos à infração até a sua regularização.

6. Eliminação dos Dados Pessoais:

Relativos à infração.

7. Suspensão Parcial do Funcionamento do Banco de Dados:
   Pelo período máximo de 6 meses, prorrogável por igual período, até a regularização da atividade de tratamento.
8. Suspensão do Exercício da Atividade de Tratamento de Dados Pessoais:
   Pelo período máximo de 6 meses, prorrogável por igual período. Proibição Parcial ou Total do Exercício de Atividades Relacionadas a Tratamento de Dados.

As sanções serão aplicadas depois dos procedimentos administrativos que possibilitem ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto, considerando os critérios:

1. A gravidade e a natureza das infrações e dos direitos pessoais afetados;
2. A boa-fé do infrator;
3. A vantagem auferida ou pretendida pelo infrator;
4. A condição econômica do infrator;
5. A reincidência;
6. O grau do dano;
7. A cooperação do infrator;
8. A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do inciso 2º do art. 48 da Lei;
9. A adoção de política de boas práticas e governança;
10. A pronta adoção de medidas corretivas;
11. A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Os vazamentos individuais ou acessos não autorizados podem ser objeto de conciliação direta entre controlador e titular. Caso não haja acordo, o controlador estará sujeito às penalidades mencionadas.

A ANPD estabelecerá, através de seu regulamento próprio, as técnicas para calcular o valor inicial das penalidades pecuniárias, as quais devem passar por consulta pública e ser divulgadas antecipadamente para conhecimento dos responsáveis pelo tratamento de dados.

E por fim, os valores arrecadados das multas aplicadas pela ANPD serão destinados ao Fundo de Defesa de Direitos Difusos conforme o inciso 5° do artigo 52 da Lei.

2.3 DADOS SENSÍVEIS

Esta seção aborda a definição de dados sensíveis segundo a LGPD e mostra a importância da segurança de tais dados com alguns exemplos de casos reais onde dados sensíveis de várias pessoas foram expostos, gerando um grande problema para os envolvidos.

2.3.1 Descrição de Dados Sensíveis segundo a LGPD

Conforme a LGPD no Art. 5°, subseção II, temos a definição de dado pessoal sensível por: " *Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.* ".

A manipulação dessas informações está sujeita a normas estritas, pois quando são divulgadas, podem ocasionar sérios prejuízos, discriminações ou danos psicológicos e também materiais, aos indivíduos que as possuem.

O artigo 11 da LGPD define as situações em que é permitido o processamento de dados sensíveis. São eles "Com Consentimento" e "Sem Consentimento".

A primeira situação descreve um cenário que o titular dos dados consente, de forma explícita e legítima, o uso de seus dados para finalidades específicas. Mas no segundo caso, o uso dos dados sensíveis só é possível sem o consentimento do titular para alguns fins específicos, conforme está descrito no Art. 11°:

1. Cumprimento de obrigação legal ou regulatória pelo controlador;
2. Tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
3. Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
4. Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei n.º 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;
5. Proteção da vida ou da incolumidade física do titular, ou de terceiro;
6. Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou vigência.
7. Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e

autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º da Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

Vale ressaltar que o inciso n.° 4 proíbe o uso de dados pessoais sensíveis para obter vantagem econômica, exceto em casos específicos de portabilidade de dados e para a adequada prestação de serviços de saúde suplementar, desde que respeitadas certas condições:

1. A portabilidade de dados quando solicitada pelo titular.
2. As transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata a seção II da Lei.

2.3.2 Casos de vazamentos de Dados sensíveis

Esta seção traz alguns exemplos de falhas de segurança referentes a dados sensíveis de empresas e organizações e algumas consequências causadas por tais vazamentos de informações.

2.3.2.1 Red Cross Blood Service

No ano de 2016, a *Red Cross Blood Service*, uma prestadora de serviços de coleta de sangue australiana, teve uma falha em seu sistema de segurança de dados expondo informações referentes a 550.000 doadores de sangue na internet (News, 2016).

De acordo com Mulholland, C. S. (2018) o fato, por si só, já seria grave, considerando a natureza pessoal dos dados que foram disponibilizados publicamente em site na Internet, quais sejam: nome, gênero, endereço e data de nascimento e também uma que era especialmente sigilosa que especificava se determinado doador seria “pessoa com comportamento sexual de risco”, informação referente a atividades sexuais de risco nos últimos 12 meses. E como pedido de desculpas, a *Red Cross* disponibilizou um aparato de atendimento às pessoas que tiveram seus dados violados.

2.3.2.2 Operação Deepwater

Em janeiro de 2021, a Polícia Federal brasileira apurou inúmeros dados sigilosos de pessoas físicas e jurídicas - tais como CPF/CNPJ, nome completo e endereço foram ilicitamente disponibilizados em um fórum na internet especializado em trocas de informações sobre

atividades cibernéticas (Polícia Federal, 2021).

Um utilizador do fórum divulgou de forma gratuita algumas informações sigilosas, mas também disponibilizou para venda outras informações confidenciais mediante o pagamento em criptomoedas.

Após várias investigações, a Polícia Federal brasileira descobriu o responsável pelos crimes de obtenção, divulgação e venda de dados, e também identificou um segundo *hacker* envolvido na venda dos dados em suas redes sociais. Além disso, foram emitidos cinco mandados de busca e apreensão e um mandado de prisão preventiva nos municípios de Petrolina–PE e Uberlândia–MG.

2.3.2.3 Netshoes

Em 2019, a Netshoes se comprometeu a pagar R$ 500,00 mil por danos morais, em acordo feito com o Ministério Público do Distrito Federal, devido à exposição na internet de dados de aproximadamente 2 milhões de clientes.

A situação ficou conhecida no começo de 2018, quando informações como nome completo, CPF, email e registro de compras foram expostos devido a erros nos sistemas da companhia.

Naquele momento, a Netshoes emitiu um comunicado à imprensa relatando que havia acionado as autoridades competentes para investigar, esclarecer e resolver o ocorrido com total transparência. A organização afirmou que a proteção de dados é um compromisso forte e que não encontrou evidências de invasão em sua rede tecnológica (Jota, 2022).

E pensando no Metaverso, a proteção de dados sensíveis é igualmente crítica. Pois há uma grande coleta de dados sensíveis, biométricos e comportamentais dos usuários, através dos formulários de criação de conta e dos sensores dos dispositivos de RV, no caso o Meta Quest que é o aparelho que possibilita a interação do mundo real com o virtual desenvolvido pela empresa Meta, veja mais no Capítulo 4.

3 TRABALHOS RELACIONADOS

Neste capítulo estão descritos os trabalhos relacionados que formaram o alicerce teórico e prático para a investigação das ameaças à privacidade e segurança de dados no Metaverso, bem como das exigências regulatórias que impactam o tratamento dessas informações. Vejamos detalhadamente cada um deles.

3.1 *Visualization and Cybersecurity in the Metaverse: A survey*

Publicado pelo *Journal of Imaging* (Chow, Y. *et al.*, 2023), o artigo apresenta questões de cibersegurança que o Metaverso enfrenta nas tecnologias de visualização que valem a pena serem mencionadas por serem muito interessantes para o objetivo desse trabalho.

Segundo o autor, as defesas contra ameaças de cibersegurança no domínio visual se tornarão cada vez mais importantes à medida que o desenvolvimento do Metaverso se torne mais maduro, pois "como se trata de uma tecnologia relativamente nova, ela ainda não recebeu muita atenção." (Chow, Y. *et al.*, 2023). Desta forma serão visualizados alguns desafios enfrentados pelo Metaverso no seu processo de desenvolvimento. Este trabalho foi divido em duas etapas:

1. Uma investigação de questões de cibersegurança, em particular, ameaças cibernéticas enfrentadas pelo Metaverso em relação ao uso de tecnologias de visualização.
2. Uma discussão sobre trabalhos existentes e direções de pesquisa abertas no desenvolvimento de contramedidas contra tais ameaças.

Durante a primeira etapa foram citadas vários trabalhos de diversos autores sobre várias categorias de ameaças de segurança e os desafios críticos encontrados em diferentes aspectos do Metaverso, e também foi apresentado um estudo sobre tecnologias de Realidade Aumentada (RA) e Realidade Virtual (RV) que não está diretamente relacionada com o metaverso em si, mas com seus métodos de acesso.

Na segunda etapa foram apresentadas questões e trabalhos referentes à segurança em RA, RV e autenticações com suas dificuldades de implementação, onde o autor faz a seguinte afirmação: "Ao contrário dos métodos tradicionais de interação por teclado, mouse ou tela sensível ao toque, os usuários de realidade estendida geralmente usam gestos, por meio de meios sem as mãos ou um controlador portátil, para realizar a entrada. Embora os gestos possam ser usados para inserir senhas de texto ou números de identificação pessoal (PINs), isso é complicado e vulnerável a ataques de observadores externos", todos esses pontos citados no artigo mostram

que o Metaverso possui muitos desafios relacionados à questão de segurança de dados sensíveis.

3.2 Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey

Neste estudo Vladimirov, I. *et al.* (2022) e os demais autores se concentraram na pesquisa e análise da segurança e privacidade da comunicação, especialmente quando informações pessoais sensíveis estão envolvidas.

Ao longo da investigação, ficou evidente que a garantia da segurança das comunicações é um desafio que se torna complexo mesmo quando técnicas de criptografia avançadas são implementadas. As comunicações frequentemente permanecem vulneráveis, e os modelos de ameaça tradicionais se mostraram inadequados para proteger informações sensíveis.

Nesse trabalho foi relatado sobre a seguinte situação: "A Internet 3.0 será eventualmente uma experiência que envolverá mais de um sentido"(Vladimirov, I. *et al.*, 2022). Isso implica que esse nível sem precedentes de imersão e interatividade tem uma consequência não intencional: um aumento na quantidade e qualidade dos riscos relacionados às tecnologias disponíveis que serão usadas para materializar a arquitetura por trás desse novo mundo digital clonado.

Esses perigos são particularmente relevantes para a privacidade e segurança de usuários e empresas que desejam operar nesse ambiente.

A necessidade de examinar minuciosamente como os dados são transferidos em ambientes digitais foi destacada pelos autores. Além disso, ressaltou-se a importância de eliminar vieses, que são erros sistemáticos no processamento da informação que se repetem de forma previsível em circunstâncias particulares (kahneman, 2012), que poderiam levar a uma adaptação inadequada ou maliciosa do mundo real, particularmente no contexto do desenvolvimento do metaverso, onde a linha entre o mundo físico e virtual é borrada.

O objetivo deste estudo foi a proteção de dados pessoais e sensíveis, e para tal, foram exploradas soluções potenciais, como a implementação de Sistemas de Detecção de Intrusão de Rede (NIDS) para combater ameaças cibernéticas e a aplicação da criptografia totalmente homomórfica, pois com ela é possível realizar um conjunto de procedimentos computacionais diretamente sobre um texto cifrado sem a necessidade de decifrá-lo, impedindo assim que a mensagem original seja de conhecimento do servidor ou de qualquer usuário que acompanhe a realização de tais procedimentos para garantir a privacidade na transferência de dados (Busatto,

2013).

Além disso, foram investigadas abordagens para proteger informações privadas durante o processo de reconstrução 3D de avatares, reconhecendo que a segurança e a privacidade desempenham um papel fundamental na garantia da segurança das operações, dos usuários e de seus avatares em um ambiente digital em constante expansão.

Em resumo, este estudo destaca a necessidade de abordar de forma abrangente a segurança e a privacidade das comunicações, especialmente à medida que as tecnologias avançam.

A proteção de dados sensíveis é um componente crítico da segurança cibernética e da integridade das interações digitais, que desempenham um papel fundamental na preservação da confidencialidade, integridade e autenticidade das informações pessoais em um mundo digital em constante evolução.

3.3 Proteção aos dados do usuário de serviços digitais pela LGPD e as cláusulas abusivas na política de privacidade

Este artigo discute a relevância da proteção dos dados pessoais, enfatizando aspectos como consentimento, transparência, venda de dados e os perigos decorrentes do mau uso de informações pessoais (Sebastião, M. P. D. A., 2022).

Casos de perigos abrangem a transgressão de direitos, intrusão na privacidade e influência por meio de métodos como a programação neurolinguística. O trabalho também destaca a anonimização como uma forma de reduzir riscos e a importância da regulamentação através da LGPD e outras legislações.

O método utilizado pela autora foi o hipotético-dedutivo e baseia-se na pesquisa documental e bibliográfica, palestras renomadas e canais de mídia de profissionais diversos. E possui o objetivo geral de demonstrar e incentivar a reflexão, inicialmente, sobre a mudança trazida pela LGPD, e logo após, com exemplos de abusos constantes na Política de Privacidade e relacionados aos dados pessoais.

Durante a primeira parte do artigo, a autora esclarece alguns pontos da LGPD que foram abordados para a sua pesquisa, e dentre eles, foi principalmente utilizado o art° VI da Lei, o qual também foi citado na Seção 2.2.

Na segunda parte do trabalho, referente aos abusos na política de privacidade, o texto discute como essas cláusulas abusivas podem prejudicar os direitos dos usuários devido à falta

de transparência e à desigualdade de poder em relação ao consumidor.

Muitas vezes, essas cláusulas se beneficiam da confiança dos usuários, principalmente em contratos de adesão, nos quais a inexperiência ou falta de informação os leva a concordar com condições que permitem acesso total aos seus dados pessoais sem respeitar seus direitos. Por fim, a autora concluiu que é crucial que o Poder Público faça uma fiscalização rigorosa para combater cláusulas abusivas nas Políticas de Privacidade, já que as fronteiras entre o mundo físico e o digital estão cada vez mais turvas.

3.4 Comparação dos trabalhos

Nessa seção teremos uma rápida comparação dos trabalhos relacionados em relação a esse trabalho, a justificativa para tal e um quadro que faz um resumo desta comparação ao final.

O trabalho da Seção 3.1 apresentou questões de segurança da informação no espaço virtual do Metaverso, ou seja, cibersegurança. Nesse contexto, a investigação realizada pelos autores sobre as características do Metaverso, sua arquitetura geral, tecnologias necessárias para seu acesso, e as ameaças à segurança e à privacidade citadas pelos autores foram utilizadas como um embasamento importante para orientar a pesquisa deste trabalho.

Na Seção 3.2 a situação relatada sobre a internet 3.0, quando se trata de informações pessoais: um escaneamento de alta definição de uma pessoa e suas características sensíveis, a confidencialidade é de extrema importância. E nesse trabalho este problema foi usado como um direcionamento para a análise dos tipos de dados que os usuários terão que disponibilizar no Metaverso, assim como consta na Seção 4.2 .

Por fim, o Trabalho da Seção 3.3 traz um estudo muito interessante sobre proteção de dados digitais oferecidos pela LGPD, que foi bastante proveitoso para a compreensão de como os dados são utilizados por empresas, o que é política de privacidade e como a LGPD regulamenta o tratamento de certos acontecimentos que afetam os usuários das plataformas digitais de todo mundo, e as mudanças significativas que ela trouxe, exigindo maior precisão e transparência nas cláusulas, com a obrigação de informar claramente como os dados serão usados.

Vejamos agora o Quadro 3 que faz uma comparação resumida sobre todos os trabalhos relacionados e o que será utilizado de cada trabalho.

Quadro 3 – Comparação entre os Trabalhos Relacionados e o Presente Trabalho

Trabalho	**Foco Principal**	**Desafios**	**Contribuição**
Visualization and Cybersecurity in the Metaverse: A Survey	Cibersegurança no Metaverso e tecnologias de acesso (RA/RV)	Vulnerabilidade em autenticação por gestos e visualizações	Investigação realizada pelos autores sobre as características do Metaverso, sua arquitetura geral, tecnologias necessárias para seu acesso, e as ameaças à segurança e à privacidade
Security and Privacy Protection Obstacles with 3D Reconstructed Models of People in Applications and the Metaverse: A Survey	Privacidade e confidencialidade de dados sensíveis no Metaverso	Riscos à privacidade e segurança em ambientes 3D	Direcionamento para analisar os tipos de dados sensíveis que serão exigidos dos usuários no Metaverso
Proteção aos dados do usuário de serviços digitais pela LGPD e as cláusulas abusivas na política de privacidade	Proteção de dados pessoais sob a LGPD e políticas de privacidade	Abuso em cláusulas de privacidade, falta de transparência	Compreensão sobre como a LGPD impacta o uso de dados no Metaverso e a exigência de transparência
Presente Trabalho	Conformidade do Metaverso da empresa Meta com a LGPD	Identificação de lacunas nas práticas de coleta, armazenamento e proteção de dados	Análise detalhada das práticas da Meta sobre proteção de dados sensíveis e sugestões de melhorias para garantir a conformidade com a LGPD.

Fonte: Elaborado pelo autor

4 METODOLOGIA

Nesta seção, abordaremos a metodologia utilizada para o estudo do metaverso desenvolvido pela empresa Meta para a aplicação chamada de *Horizon Worlds*, uma plataforma de VR que permite que os usuários criem e explorem ambientes virtuais imersivos em 3D, interajam socialmente e participem de atividades em um espaço virtual compartilhado. E utilizando as informações da plataforma oficial da empresa Meta[1], para avaliar a coleta de dados na criação da conta Meta com o propósito de identificar e analisar problemas do espaço virtual com a aplicação das normas estabelecidas pela LGPD.

A escolha da Meta e do *Horizon Worlds* se justifica pela sua relevância no cenário atual de plataformas de metaverso e pelo volume de dados pessoais sensíveis que essa aplicação coleta.

E também durante o processo, a análise foi limitada pela falta de acesso físico ao dispositivo *Meta Quest*, e que as políticas de privacidade podem variar ao longo do tempo. Em futuras pesquisas, uma validação por especialistas em direito digital e proteção de dados poderia enriquecer a análise realizada.

Começando pela Seção 4.1 foi realizada uma análise documental dos processos de coleta e tratamento de dados na criação da conta Meta, onde foram observados os procedimentos de coleta dos dados dos usuários, finalidade dos dados e consentimento do usuário sobre a utilização dos dados.

A pesquisa também examinou na Seção 4.2 os tipos de dados coletados pelos dispositivos *Meta Quest*, que permitem a interação com o *Horizon Worlds*. Utilizando informações disponíveis no site oficial do *Meta Quest*[2], uma vez que o dispositivo não estava disponível para análise física.

A seguir, na Seção 4.3, foi realizada uma análise de conteúdo das políticas de privacidade do *Horizon Worlds*[3], com foco nas práticas de coleta e uso de dados sensíveis, como o rastreamento ocular e de expressões faciais, além de dados de atividades.

E, por fim, foi realizado um levantamento dos procedimentos recomendados pela LGPD na Seção 4.4, a fim de observar a base legal sobre a coleta de dados e os direitos dos titulares.

---

[1] Disponível em https://about.meta.com/br/

[2] Disponível em https://www.meta.com/quest/

[3] Disponível em https://www.meta.com/pt-br/help/quest/articles/horizon/safety-and-privacy-in-horizon-worlds

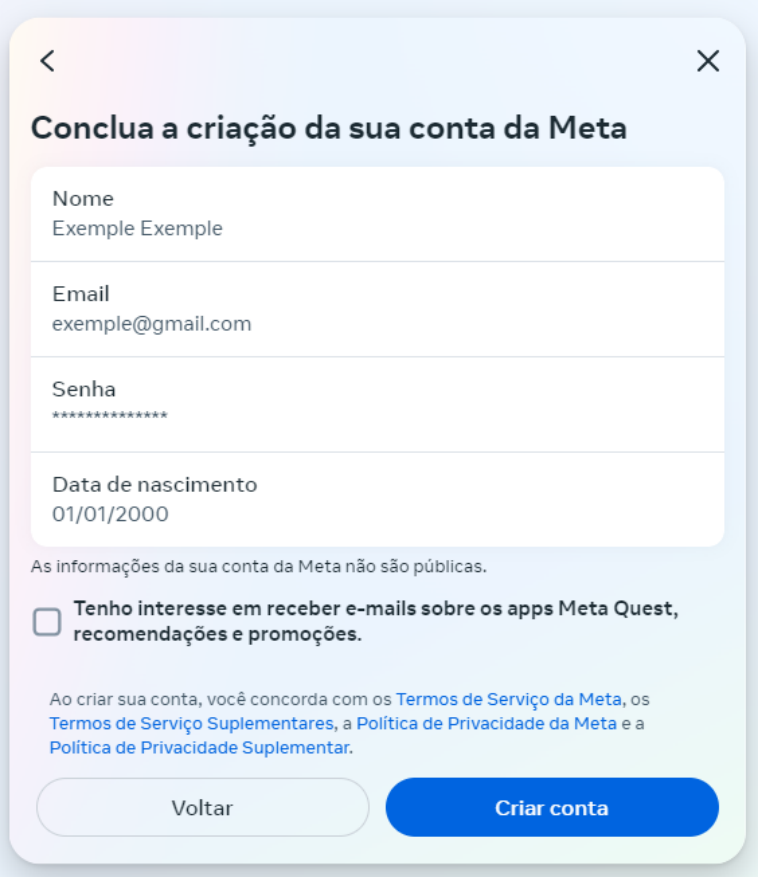
Para avaliar a conformidade com a LGPD, foram utilizados os Quadros 1 e 2, que descrevem os direitos garantidos aos titulares de dados e o ciclo de vida dos dados, respectivamente. A partir desses quadros, examinamos a coleta e tratamento de dados nas capturas de tela da plataforma Meta e comparamos esses procedimentos com as disposições legais para obter os resultados no Capítulo 5.

4.1 Análise dos processos de coleta e tratamento de dados na criação da conta Meta

O Processo de análise utilizado segue a seguinte ordem de estudo: Coleta, Finalidade e Consentimento.

1. **Coleta**: Foi Inicialmente observado a forma em que os dados dos usuários são coletados pela plataforma e também quais dados são utilizados nessa coleta.
   E antes de Iniciar efetivamente na plataforma *Horizon Worlds* é necessário a criação de uma conta na plataforma Meta, onde dados são coletados para tal. Veja a Figura 3.

Figura 3 – Captura de Imagem na plataforma Meta na tela de criação de Conta

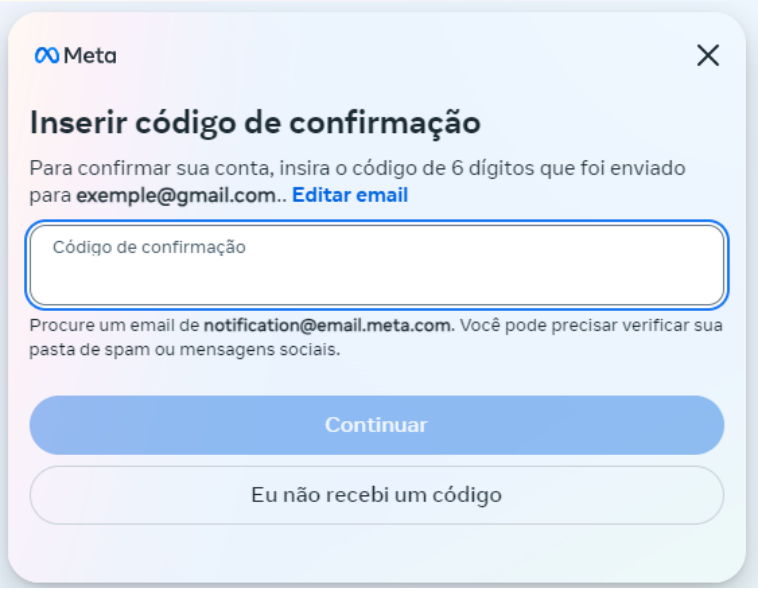


Fonte: Elaborado pelo autor

Após a coleta, foi realizada também uma verificação de email como medida de segurança

adicional. Veja a Figura 4.

Figura 4 – Captura de Imagem na plataforma Meta na tela de Verificação de Email



Fonte: Elaborado pelo autor

E seguida a verificação de email, foram requisitadas mais algumas informações para a plataforma, que consistem nos nomes que o usuário utilizará na plataforma.

E durante esse processo alguns detalhes podem ser levados em consideração nessa etapa, pois os nomes escolhidos pelo usuário possuem diferentes usos:

a) Nome Público: Primeiro é escolhido o nome público do usuário que é visível a todas as pessoas dentro da plataforma, e pode ser utilizados por outras pessoas também. Além disso, este nome pode ser um nome falso ou não, e pode ser alterado a qualquer momento.

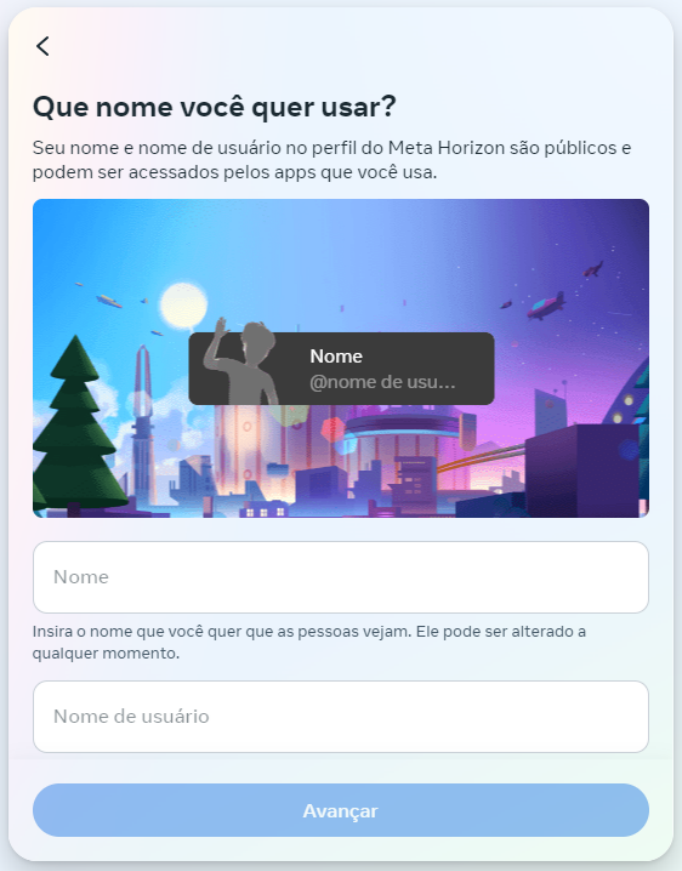
b) Nome de Usuário: Este segundo é um pouco diferente, pois deve ser único e só pode sofrer alteração a no mínimo de 6 meses.Veja a Figura 5.

E para finalizar a criação da conta, o usuário escolhe que tipo de visibilidade sua conta terá, ela pode ser aberta a todos, à família e amigos, e pessoal ou solo.

Cada opção traz um diferente nível de controle de visualização da conta, isso implica em segurança virtual e exposição de dados a públicos diferentes e um alcance maior ou menor de pessoas.

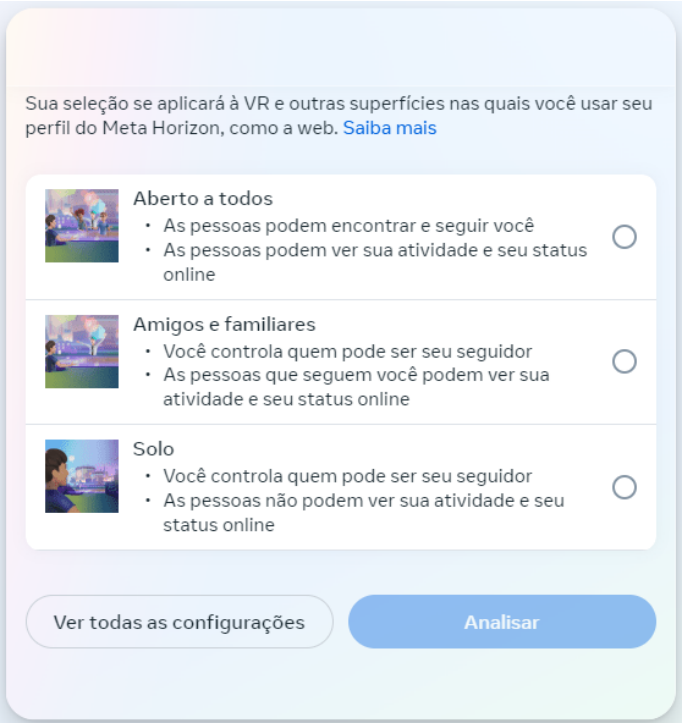
Nesse ponto podemos observar que o próprio usuário tem o direito de escolher a maneira que seus dados podem ser tratados no que se refere a publicidade. Veja os detalhes nas Figuras 6 e 7.

Figura 5 – Captura de Imagem na plataforma Meta na tela de Criação de Nomes de Usuário



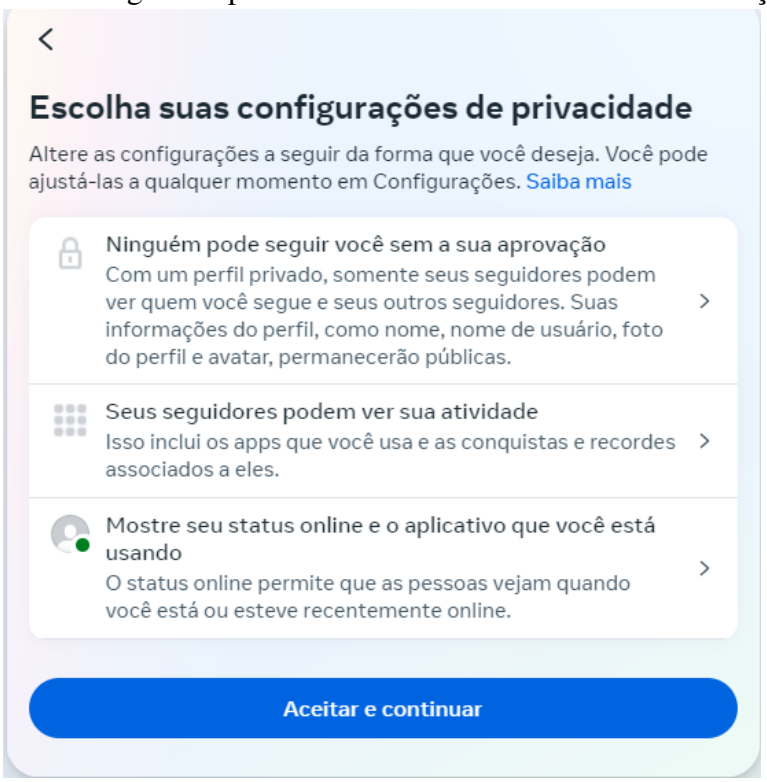
Fonte: Elaborado pelo autor

Figura 6 – Captura de Imagem na plataforma Meta na tela visibilidade



Fonte: Elaborado pelo autor

Figura 7 – Captura de Imagem na plataforma Meta na tela visibilidade avançada



Fonte: Elaborado pelo autor

Até o momento, todas as informações foram coletadas por meio de formulários, onde o usuário tem total liberdade para escolher as informações que serão públicas e privadas na plataforma Meta.

2. **Finalidade das informações**

Para verificar as finalidades das informações coletadas primeiro iremos listá-las:

a) Nome
b) Email
c) Senha
d) Data de nascimento
e) Nome público
f) Nome de usuário
g) Tipo de visibilidade da conta

Quando analisamos a Figura 3 podemos observar que a plataforma deixa claro que os dados ali utilizados para a criação da conta não serão públicos, ou seja, o nome pessoal, email, data de nascimento. Pois a plataforma só é permitida para maiores de 18 anos no Brasil, e senha do usuário serão utilizados com intuito de criar a conta Meta.

Mas quando analisamos a Figura 5, podemos observar que as informações dessa etapa de

criação da conta agora serão públicas, ou seja, outras pessoas terão acesso a elas. Isso nos remete que a finalidade dessas informações são para exibição pública. São elas o Nome público e o de Usuário

Por fim, ao analisar as Figuras 6 e 7 observamos que a finalidade desta etapa refere-se à maneira de exibição da própria conta e o alcance que ela terá para ser encontrada por outras pessoas.

3. **Consentimento**:

   Durante todo o procedimento de criação da conta, está explicitamente escrito que ao criar a conta o usuário está concordando com as medidas de privacidade da empresa Meta, observe a Figura 3 e 7.

4.2 Análise sobre os tipos de dados coletados no aparelho *Meta Quest* e sua utilização

Durante a criação da conta Meta, todos os dados utilizados foram coletados por formulários de texto, entretanto, agora temos um certo avanço no que se diz respeito à coleta de informações, pois elas deixaram de ser escritas e agora tratamos de informações em tempo real utilizando sensores presentes no *Meta Quest*.

O *Meta Quest* é o aparelho que possibilita a interação do mundo real com o virtual da empresa Meta, trata-se de um óculos de VR onde alguns contam com controles joysticks para as mãos e outros mais avançados possuem leitores de rastreio ocular.

Por questões de não acesso ao aparelho físico, as informações utilizadas foram obtidas do site oficial do *Meta Quest*.

Começando pelos sensores do aparelho temos:

1. **Microfone:** Este é um sensor comumente usado pela maioria dos aparelhos digitais atualmente, e para o uso dele no *Meta Quest* é requisitado ao usuário o acesso ao microfone, isto implica que ao permitir tal ação o usuário estará permitindo o uso do microfone de seu aparelho VR, para gravações de áudio e também de voz.
2. **Localizador:** Conforme a versão VR, será solicitado que você permita que o app acesse sua localização. E o usuário pode escolher se deseja ou não permitir o acesso. Segundo o site, estas informações são utilizadas, por exemplo, para que um app de compras exibisse sua moeda e preços locais. Entretanto, este recurso se utilizado de maneira indevida pode acarretar problemas ao usuário, principalmente para crianças, contudo, as contas da Meta para crianças entre 10 e 12 anos só podem compartilhar dados de localização aproximados

com os aplicativos.

3. **Sensor de rastreamento corporal:** Este recurso quando ativado permite que o dispositivo colete dados sobre a posição do corpo e das mãos do usuário, e também o tamanho estimado das mãos e a escala corporal do mesmo. As imagens do corpo e das mãos são analisadas no dispositivo em tempo real e, por questões de segurança do usuário, excluídas após o processamento e não são armazenadas nos servidores da Meta.
4. **Rastreamento ocular:** Este recurso só está disponível para a versão *Meta Quest* Pro, ela procura dar ao avatar um contato visual e movimento facial mais natural e melhorar a qualidade visual na área onde está olhando na VR. Além de possibilitar a utilização dos olhos do usuário como método de entrada, semelhante ao mouse de computador, isso significa que a interação com o conteúdo virtual pode ser feito com base em onde está se olhando. Como medida de segurança, os dados brutos de imagem dos olhos não são compartilhados com aplicativos, mesmo permitido o acesso aos dados do rastreamento ocular.
5. **Rastreamento de expressões faciais:** Semelhante ao Rastreamento Ocular, esse recurso está disponível apenas para a versão *Meta Quest* Pro, além disso, os dados brutos de imagem não são compartilhados com aplicativos, e tem objetivo de naturalizar as expressões faciais do usuário para utilização nos aplicativos.
6. **Armazenamento:** Se um aplicativo solicitar acesso para ler ou escrever no armazenamento compartilhado do dispositivo *Meta Quest*, por exemplo, para baixar e salvar arquivos de mídia, incluindo fotos e vídeos criados.

Estes são os sensores cruciais dos dispositivos VR *Meta Quest*, mas que informações podem ser requisitadas pelos aplicativos?

Os apps podem solicitar dados vinculados às atividade do app e identificadores pessoais. Tais como:

1. Número de identificação do usuário: Se um app solicitar acesso ao número de identificação do usuário.
2. Faixa etária: Se um app solicitar acesso à faixa etária para garantir uma experiência adequada à idade.
3. Perfil do usuário: Se um app solicitar acesso ao perfil de usuário do *Meta Quest*, isto é, nome de usuário e foto do perfil.
4. Avatar: Se um app solicitar acesso ao avatar.

5. Seguidores: Se um app solicitar acesso aos seguidores.
6. Dados de uso: Se um app solicitar acesso aos dados sobre a atividade no app. Os dados de uso podem incluir, entre outras coisas, informações sobre as assinaturas, convites, combinações, grupos, salas, desafios e funcionalidades.
7. Dados espaciais: Se um app solicitar dados sobre o espaço físico. Quando alguém fornece acesso aos dados espaciais, os apps podem coletar dados sobre o conteúdo do espaço físico, por exemplo, mesa, sofá, janelas, bancada. Isso significa que os personagens e os objetos de experiências combinadas podem aparecer dentro, em cima e em volta dos objetos no espaço como se estivessem realmente lá.
8. Destinos: Se um app solicitar dados sobre os destinos visitados. Os destinos fazem parte de um app e incluem localizações, níveis ou modos individuais, bem como servidores multijogador, artigos de mídia e outros objetos de interesse destinados ao compartilhamento que foram especificados pelo recurso Destinos.

Finalizada a análise de informações sobre os sensores do *Meta Quest* e as informações de Apps com seus usos, iniciamos o estudo sobre as políticas de Privacidade no app*Horizon Worlds*.

4.3 Análise das Políticas de Privacidade no app *Horizon Worlds*

Compreender a política de privacidade do *Horizon Worlds* é crucial para que os usuários possam proteger suas informações pessoais. Lançado oficialmente em 2021, a aplicação permite que os usuários criem, explorem e interajam em mundos virtuais compartilhados(Meta, 2024).

Este aplicativo utiliza os seguintes sensores: Armazenamento, Expressões faciais, Rastreamento ocular e Microfone.

E coleta as seguintes informações: Número de identificação do usuário, perfil do usuário, Avatar, Seguidores, Dados de uso e faixa etária.

Segundo Meta (2024) a aplicação conta com muitos recursos de proteção de dados como criptografia, controles de acesso e monitoramento de atividades suspeitas. E um recurso em específico que vale ser mencionado é o Código de Conduta para Experiências Virtuais (CCVE).

4.3.1 Código de Conduta CCVE

Esse código de conduta considera alguns conteúdos inadequados à comunidade e que estes podem prejudicar gravemente a experiência de outros usuários na plataforma, como:

1. Fingir ser outra pessoa ou entidade, roubar a identidade de alguém ou criar, ou usar contas falsas.
2. Envolver-se em fraudes, golpes ou outras atividades enganosas.
3. Coletar ou compartilhar informações pessoais sensíveis, fazer doxing (revelar e/ou vazar informações sigilosas e pessoais) com outras pessoas, comprometer contas de usuários, compartilhar informações de login de contas, obter acesso não autorizado ou compartilhar malware.
4. Criar ou usar uma conta da Meta que não seja destinada à sua idade.

O Código também abrange outras categorias de problemas que promovem ou podem causar danos físicos, como:

1. Sexualizar, explorar ou abusar de menores de idade.
2. Praticar bullying, assédio, perseguição, comportamento de ódio ou xenofóbico.
3. Defender, envolver-se ou promover a violência, a exploração humana, o tráfico de pessoas ou o contrabando de migrantes. Apoiar ou representar grupos, ou indivíduos envolvidos em terrorismo, organizações baseadas no ódio ou grupos criminosos
4. Qualquer forma de atividade íntima não consensual, incluindo o compartilhamento de imagens íntimas de outras pessoas sem consentimento.
5. Venda, troca ou promoção ilegal de produtos regulamentados.

Estes são apenas alguns exemplos de problemas que podem acontecer, e por ventura, serão seriamente punidos pela Meta em caso de confirmação. Segundo o site da empresa: “Espaços públicos como lobbies abertos, jogos multijogadores e eventos públicos criam oportunidades especiais para públicos amplos”. Isto implica dizer que nem mesmo a própria empresa terá total controle sobre as pessoas que irão acessar a plataforma.

Além do código de conduta, os desenvolvedores, e como os criadores e administradores de apps, também podem estabelecer suas próprias regras, para uma maior abrangência de segurança para os usuários.

4.3.2 Controle de Atividade

Outras configurações de privacidades podem ser observadas dentro da aplicação, é possível controlar quem vê a atividade, ou seja, os apps que ativam o status online mostrando quando o usuário está ou esteve online recentemente.

As atividades também incluem outras plataformas onde o perfil do Meta Horizon é usado. Elas podem ser compartilhadas para os seguintes públicos:

1. Público, ou seja, todos podem ver sua atividade.
2. Seus seguidores, somente as pessoas que seguem você podem ver sua atividade.
3. Somente eu, apenas o usuário pode ver a própria atividade, entretanto, mesmo com esta opção selecionada, a atividade em apps específicos pode ficar visível para outras pessoas, por exemplo, existe a possibilidade do nome ser exibido em quadros de líderes ou receber uma recomendação para se conectar com alguém que jogou o mesmo jogo.

Durante a atividade no app, é possível desativar a opção: “Status online”. Esta opção possibilita mostrar quando se está ou esteve online recentemente na VR e em outras plataformas compatíveis com o perfil do Meta Horizon, além disso, quando desativada, o usuário não poderá ver o status online de outras pessoas.

Entretanto, mesmo com essa opção desativada, a presença em apps específicos do usuário continuará sendo mostrada a outras pessoas que estiverem usando o mesmo app, isto é o seu avatar. Intencionalmente ou não, enquanto se usa o app, não apenas informações são compartilhadas com o usuário, mas ele também compartilha informações com outras pessoas. Pensando nessa possibilidade, o usuário pode optar por compartilhar dados adicionais ou não.

Os dados adicionais em sua maioria são para melhorar a experiência de produto Meta, e para melhorar o desempenho do app e dos recursos. Esta escolha será aplicada aos seguintes apps e recursos: Sistema operacional (OS), Loja, Navegador, Explorar, Configurações, Recursos sociais e Messenger, Espaço, Eventos, Arquivos, TV, Placares, *Meta Quest* Move.

4.4 Análise dos processos de coleta e tratamento de dados segundo as regulamentações da LGPD

Nesta seção foi realizado um levantamento dos procedimentos recomendados pela LGPD, a fim de observar a base legal sobre a coleta de dados e os direitos dos titulares.

4.4.1 Bases Legais para o Tratamento de Dados

Segundo o Serviço Federal de Processamento de Dados (Serpro) existem 10 princípios para o tratamento de dados pessoais, veja a Figura 8, e que a base da LGPD é o consentimento: ou seja, é necessário solicitar a autorização do titular dos dados, antes do tratamento ser realizado. E esse consentimento deve ser recebido de forma explícita e inequívoca.

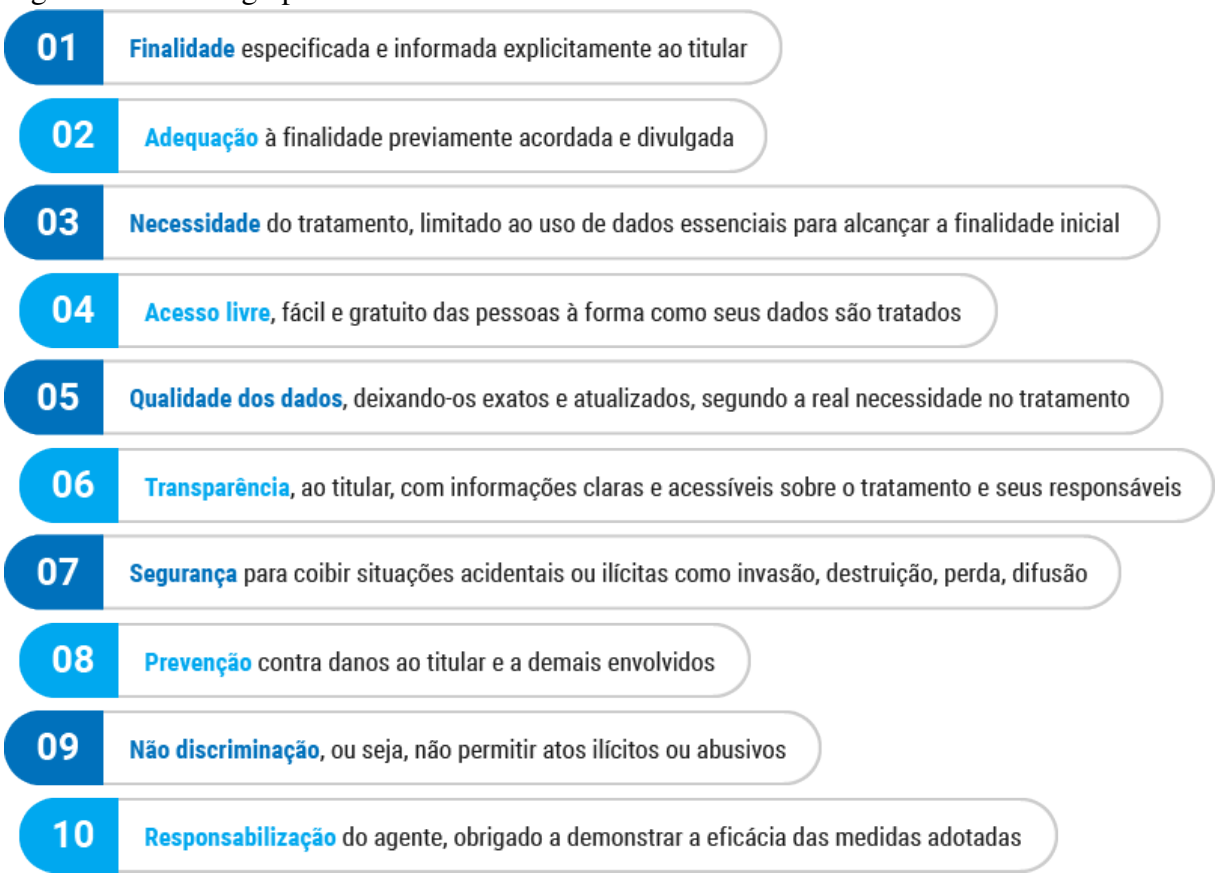
Conforme o Art. 7º da LGPD, o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

1. Mediante o fornecimento de consentimento pelo titular.
2. Para o cumprimento de obrigação legal ou regulatória pelo controlador.
3. Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.
4. Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
5. Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.
6. Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.
7. Para a proteção da vida ou da incolumidade física do titular, ou de terceiro.
8. Para a tutela da saúde, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
9. Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.
10. Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O não consentimento é a exceção: só é possível processar dados, sem autorização do cidadão, quando isso for indispensável para cumprir situações legais, previstas na LGPD e/ou em legislações anteriores, como a Lei de Acesso à Informação (LAI).

Por exemplo, uma organização - pública ou privada - pode, sem precisar pedir novo consentimento, tratar dados tornados anterior e manifestamente públicos pelo cidadão. Isso está alinhado com o Art. 7º, seção 4º da lei, que dispensa a exigência de consentimento para dados tornados manifestamente públicos pelo titular.

Figura 8 – Decálogo para um tratamento de dados efetivo



Fonte: Adaptado de Serpro (2024)

5 RESULTADOS

Finalizada as análises sobre as práticas de coletas de dados do *Horizon Worlds* e as exigências da LGPD, veremos algumas comparações sobre a utilização de dados nos mesmos e os resultados destas comparações.

O Quadro 4 detalha os sensores do dispositivo e os dados que eles coletam, com suas finalidades. Ele lista sensores como microfone, localizador e rastreamento corporal, explicando que, por exemplo, o microfone grava áudio para comandos de voz, enquanto o localizador coleta dados de localização para personalizar a experiência do usuário. O quadro também destaca que os dados de rastreamento corporal e facial são utilizados para proporcionar interações naturais, com a garantia de que informações sensíveis não são armazenadas ou compartilhadas.

Quadro 4 – Dados Coletados pelo Meta Quest

Sensor	**Dado Coletado**	**Finalidade**
Microfone	Gravações de áudio e voz.	Permitir a interação por meio de comandos de voz e gravação de áudio.
Localizador	Dados de localização.	Exibir moeda e preços locais nos aplicativos, garantindo a personalização da experiência.
Sensor de rastreamento corporal	Posição do corpo, das mãos e escala corporal.	Proporcionar uma interação natural e imersiva, excluindo dados após o processamento para segurança.
Rastreamento ocular	Dados de movimento ocular.	Melhorar a qualidade visual e permitir interação através do olhar, sem compartilhamento de dados brutos.
Rastreamento de expressões faciais	Dados de expressões faciais.	Naturalizar expressões faciais em aplicativos, sem compartilhamento de dados brutos.
Armazenamento	Acesso a arquivos de mídia.	Permitir que aplicativos leiam e escrevam no armazenamento do dispositivo, como fotos e vídeos.

Fonte: Elaborado pelo autor com informações do site oficial do Meta Quest.

O Quadro 5 mostra a comparação entre os princípios da LGPD e as práticas de coleta de dados da Meta no *Horizon Worlds*. Cada princípio da LGPD é acompanhado pela prática correspondente da Meta, demonstrando como a empresa adota ou deve adotar ações para garantir conformidade. Dando um exemplo, o consentimento do dono da conta é claramente dado ao criar uma conta Meta, assegurando que os usuários estejam informados sobre como seus dados e sensores, como microfone e rastreamento ocular, serão usados.

Quando necessário cumprir obrigações legais ou regulatórias, a Meta solicita dados como a data de nascimento para estar conforme as leis de proteção à infância. As áreas de administração pública ou proteção de crédito serão tratados na Seção 5.1.

Quadro 5 – Comparação entre os termos do Art. 7° da LGPD e as práticas de coleta de dados do *Horizon Worlds*

Prática	**LGPD**	**Meta**
Consentimento do titular	A coleta e o uso de dados pessoais devem ser consentidos explicitamente pelo titular.	Durante a criação da conta Meta, o usuário dá seu consentimento explícito para o uso dos dados, conforme mostrado na Figura 3. Além disso, há consentimento para o uso de sensores no *Meta Quest*, como microfone e rastreamento ocular.
Cumprimento de obrigação legal ou regulatória	O controlador pode tratar dados para cumprir obrigações legais ou regulatórias.	A criação da conta exige informações como data de nascimento para garantir que o usuário seja maior de 18 anos, cumprindo assim a legislação de proteção ao menor.
Administração pública	Dados podem ser tratados para execução de políticas públicas.	Não se aplica diretamente ao *Horizon Worlds*, pois é uma plataforma privada. No entanto, a Meta deve cumprir as leis de cada país em que opera.
Estudos por órgão de pesquisa	Dados podem ser usados para pesquisa, garantida a anonimização.	Não mencionado diretamente, mas a Meta pode usar dados anonimizados para melhorar a experiência do usuário e desenvolver novos produtos.
Execução de contrato	Dados podem ser tratados para execução de contrato.	A criação e manutenção da conta Meta envolvem um contrato de adesão entre o usuário e a Meta, permitindo o uso dos dados para a prestação do serviço.
Exercício regular de direitos	Dados podem ser usados em processos judiciais ou administrativos.	A política de privacidade da Meta menciona que os dados podem ser usados para proteger os direitos da empresa em caso de litígios.
Proteção da vida ou da incolumidade física	Dados podem ser tratados para proteger a vida e a segurança.	O controle de atividade no *Horizon Worlds* pode prevenir abusos e comportamentos prejudiciais, protegendo a segurança dos usuários.
Tutela da saúde	Dados podem ser usados para procedimentos de saúde.	Não se aplica ao *Horizon Worlds*.
Interesses legítimos	Dados podem ser tratados para atender interesses legítimos do controlador ou de terceiros.	A coleta de dados no *Horizon Worlds* e no *Meta Quest* é justificada pelos interesses legítimos da Meta em melhorar seus produtos e serviços, desde que não violem os direitos dos usuários.
Proteção do crédito	Dados podem ser usados para proteger o crédito.	Não se aplica diretamente ao *Horizon Worlds*, mas a Meta deve garantir a segurança financeira das transações na plataforma.

Fonte: Elaborado pelo autor

O Quadro 6 contrasta a coleta de dados do *Horizon Worlds* com os direitos dos titulares de dados conforme a LGPD. A Meta garante que os dados dos usuários são processados conforme os propósitos legítimos e informados, mediante consentimento explícito. A obtenção

de informações está segundo os objetivos estabelecidos, com dados constantemente atualizados e pertinentes.

A Meta fornece informações sobre o tratamento de dados de forma fácil e gratuita, assegurando transparência e segurança por meio de medidas técnicas e administrativas. Adicionalmente, ela implementa ações preventivas para evitar danos e assegura que os dados não serão utilizados de maneira discriminatória e assume a responsabilidade pelo processamento dos dados e implementa ações para assegurar a conformidade com as leis de proteção de dados pessoais.

A seguir, o Quadro 7 mostra as etapas do ciclo de vida dos dados no*Horizon Worlds*, conforme as atividades de processamento estabelecidas pela LGPD. Durante a fase de coleta, a Meta adquire informações pessoais ao se criar a conta e ao utilizar os sensores no *Meta Quest*. A etapa de retenção consiste em armazenar de forma segura essas informações em bancos de dados eletrônicos.

O processamento envolve a análise e utilização dos dados para personalizar serviços e criar produtos inovadores. No compartilhamento, informações são enviadas a parceiros e terceiros autorizados para objetivos específicos. Por fim, durante a etapa de eliminação, as informações são excluídas de maneira segura assim que não são mais necessárias ou mediante solicitação do usuário, assegurando o descarte apropriado.

Por fim, o Quadro 8 apresenta um checklist das principais métricas da LGPD atendidas, não atendidas ou não aplicáveis pela Meta. Esse quadro permite verificar o grau de conformidade da Meta em relação aos princípios da LGPD, destacando as práticas adotadas pela empresa no gerenciamento de dados sensíveis dos usuários.

Por exemplo, o consentimento do titular é claramente atendido, como visto ao criar uma conta Meta, onde os usuários são informados sobre o uso de seus dados, incluindo sensores como microfone e rastreamento ocular. No caso de cumprimento de obrigação legal ou regulatória, a Meta também está em conformidade, coletando dados como a data de nascimento para cumprir com leis de proteção infantil.

Algumas práticas, como administração pública, tutela da saúde e proteção de crédito, são classificadas como não aplicáveis, refletindo áreas em que a Meta não atua diretamente no tratamento de dados. Já em outros aspectos, como a proteção da vida, o exercício regular de direitos e os interesses legítimos, a Meta segue conforme as diretrizes da LGPD, garantindo a segurança e a integridade dos dados dos titulares.

Quadro 6 – Comparação entre práticas de coleta de dados do *Horizon Worlds* e os direitos garantidos aos titulares de dados pela LGPD referentes ao Quadro 1

Direitos dos Titulares	**Prática no *Horizon Worlds***	**Referência Legislativa (LGPD)**
Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades	A Meta informa explicitamente ao usuário durante a criação da conta sobre os propósitos específicos e explícitos para o uso dos dados, obtendo consentimento.	Art. 6º, I
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	A coleta de dados pela Meta é feita de acordo com as finalidades informadas, garantindo compatibilidade com o contexto do uso do *Horizon Worlds*.	Art. 6º, II
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	A Meta coleta apenas os dados necessários para a prestação dos serviços no *Horizon Worlds*, conforme informado aos usuários.	Art. 6°, III
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais	A Meta oferece aos usuários acesso facilitado e gratuito às informações sobre o tratamento e a duração do uso dos seus dados pessoais.	Art. 6º, IV
Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento	A Meta se compromete a manter os dados dos usuários atualizados, precisos e relevantes para a finalidade de uso no *Horizon Worlds*.	Art. 6º, V
Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial	A Meta proporciona informações claras e precisas sobre o tratamento dos dados e os agentes envolvidos, respeitando os segredos comercial e industrial.	Art. 6º, VI
Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão	A Meta adota medidas técnicas e administrativas para garantir a segurança dos dados dos usuários contra acessos não autorizados e situações de destruição, perda, alteração ou difusão.	Art. 6º, VII
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais	A Meta implementa medidas preventivas para evitar danos aos dados dos usuários decorrentes do tratamento no *Horizon Worlds*.	Art. 6º, VIII
Direito de não ser discriminado de forma ilícita ou abusiva	A Meta garante que os dados dos usuários não serão usados de forma discriminatória, ilícita ou abusiva.	Art. 6º, IX
Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais	A Meta se responsabiliza e presta contas pelo tratamento dos dados dos usuários, adotando medidas eficazes para garantir a conformidade com as normas de proteção de dados pessoais.	Art. 6º, X

Fonte: Elaborado pelo autor

Quadro 7 – Ciclo de vida dos dados no *Horizon Worlds*

Fase do Ciclo	**Descrição no *Horizon Worlds***	**Operações de Tratamento - LGPD, ART. 5º, X**
Coleta	Obtenção de dados pessoais dos usuários durante a criação da conta, uso de sensores no *Meta Quest* (como microfone e rastreamento ocular), e interação na plataforma *Horizon Worlds*.	Coleta, produção, recepção.
Retenção	Armazenamento seguro dos dados pessoais dos usuários em bancos de dados eletrônicos, garantindo a disponibilidade e integridade dos dados enquanto necessário para os propósitos informados.	Arquivamento e armazenamento.
Processamento	Análise e uso dos dados para melhorar a experiência do usuário, personalização dos serviços, desenvolvimento de novos produtos e funcionalidades, e para avaliação e controle da informação.	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação.
Compartilhamento	Transmissão de dados para parceiros e terceiros autorizados para fins específicos, como melhoria dos serviços, publicidade personalizada e cumprimento de obrigações legais.	Transmissão, distribuição, comunicação, transferência e difusão.
Eliminação	Remoção segura dos dados pessoais dos usuários após o término do uso conforme os propósitos informados ou a pedido do usuário, assegurando o descarte correto dos dados.	Eliminação.

Fonte: Elaborado pelo autor

Quadro 8 – Checklist das Métricas da LGPD atendidas, não atendidas ou não aplicáveis pela Meta

Base Legal da LGPD	**Status**	**Justificativa**
Consentimento do titular	Atendido	...
Cumprimento de obrigação legal ou regulatória	Atendido	...
Administração pública	Não aplicável	A Meta é uma empresa Privada.
Estudos por órgão de pesquisa	Atendido	...
Execução de contrato	Atendido	...
Exercício regular de direitos	Atendido	...
Proteção da vida ou da incolumidade física	Atendido	...
Tutela da saúde	Não aplicável	A Meta não coleta dados relacionados a saúde dos usuários nesta aplicação.
Interesses legítimos	Atendido	...
Proteção do crédito	Não aplicável	A finalidade dessa base é garantir que em situações de cobrança ou dívidas contraídas, os titulares não usem os mecanismos da LGPD como brecha para escaparem de suas obrigações financeiras.

Fonte: Elaborado pelo autor

5.1 Melhorias e Soluções para Práticas de Coleta de Dados do *Horizon Worlds*

Como consequência de algumas práticas da LGPD que não se aplicavam ao *Horizon Worlds* diretamente, como visto no Quadro 5, aqui estão listados alguns possíveis pontos de melhorias para a plataforma.

1. Administração Pública:

   Estabelecer um time especializado em monitorar as leis locais e trabalhar em conjunto com autoridades governamentais para assegurar que as atividades da Meta estejam conforme com as políticas e regulamentações de cada país em que atua.

2. Proteção de crédito:

   Dentro do *Horizon Worlds* é possível fazer compras no app, isto significa que a Meta deve garantir que todas as transações financeiras realizadas dentro da plataforma sejam seguras e protegidas contra fraudes.

   Para proteger os dados do usuário durante as compras pode ser utilizado, por exemplo, criptografia de ponta a ponta, tokens de confirmação, auditorias, etc.

6 CONCLUSÕES E TRABALHOS FUTUROS

A presente pesquisa teve como objetivo geral identificar a adequação do Metaverso desenvolvido pela empresa Meta com as normas de segurança de dados da Lei Geral de Proteção de Dados (LGPD).

A comparação entre as práticas adotadas pela Meta e os princípios da LGPD revelou que a empresa já adota práticas em consonância com a legislação brasileira. Entretanto, ainda existem lacunas em relação à conformidade plena com as exigências da LGPD.

As principais inconformidades foram identificadas em áreas como a administração pública, o uso de dados para pesquisas e a proteção de crédito. Embora não sendo diretamente aplicadas no ambiente virtual, a ausência de políticas claras e específicas para lidar com esses aspectos pode resultar em riscos significativos para a privacidade e segurança dos dados dos usuários.

Essas inaplicabilidades representam áreas para a melhoria contínua, destacando a importância de uma revisão constante das práticas de segurança e proteção de dados pessoais na evolução do Metaverso. Assim, este trabalho contribui para o entendimento das complexidades envolvidas na adequação de novas tecnologias às regulamentações existentes, fornecendo uma base sólida para futuros estudos e aprimoramentos na área de proteção de dados.

Um exemplo significativo seria a condução de uma análise comparativa entre a conformidade da plataforma Meta com a LGPD e outras legislações internacionais de proteção de dados, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e a Lei de Privacidade do Consumidor da Califórnia (CCPA).

Essa análise comparativa poderia identificar diferenças e semelhanças nas abordagens de conformidade, oferecendo perspectivas sobre como empresas globais podem desenvolver estratégias universais de proteção de dados.

Esses estudos complementares podem contribuir significativamente para a criação de um ambiente digital mais seguro e segundo as exigências legais, promovendo um uso ético e responsável do Metaverso à medida que ele continua a evoluir e expandir.

REFERÊNCIAS

Brasil, G. D. d. **Guia LGPD**. 2020. https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 22 jun. 2023.

Brasil, G. D. do. **Portal do Governo do Brasil - Acesso à Informação - LGPD**. 2018. https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd. Acesso em: 23 jun. 2023.

Busatto, N. J. **Criptografia Homomórfica**. 49 p. Monografia de Graduação — Departamento de Engenharia Elétrica, Universidade de Brasília, DF, 2013. Disponível em: https://bdm.unb.br/bitstream/10483/15372/1/2013_NarcisoBusattoJunior.pdf. Acesso em: 02 out. 2024.

Cheng, R.; Wu, N.; Chen, S.; Han, B. Will metaverse be nextg internet? vision, hype, and reality. **IEEE Network**, v. 36, n. 5, p. 197–204, 2022. Disponível em: https://ieeexplore.ieee.org/document/9877927. Acesso em: 20 set. 2023.

Chow, Y.; Susilo, W.; Li, Y.; Li, N.; Nguyen, C. Visualization and cybersecurity in the metaverse: A survey. **Journal of Imaging**, v. 9, n. 1, 2023. ISSN 2313-433X. Disponível em: https://www.mdpi.com/2313-433X/9/1/11. Acesso em: 28 jun. 2024.

CodeCrush. **Metaverso: O que é, como funciona e o que esperar desta tecnologia?** 2022. Disponível em: https://codecrush.com.br/blog/metaverso. Acesso em:02 09 2024.

Eno, J.; Gauch, S.; Thompson, C. Searching for the metaverse. In: **Proceedings of the ACM Symposium on Virtual Reality Software and Technology**. Kyoto, Japan: Association for Computing Machinery, New York, United States, 2009. Disponível em: https://dl.acm.org/doi/10.1145/1643928.1643976. Acesso em: 20 jan. 2024.

Fernandez, C. B.; Hui, P. Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse. In: **2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW)**. Las Vegas, NV, USA: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022. p. 272–277. Disponível em: https://ieeexplore.ieee.org/document/9951378. Acesso em: 20 set. 2023.

Ferreira, L.; Okano, M. T.; Aguiar, F.; De Castro Lobo dos Santos, H.; Ursini, E. L. A panorama of the implementation of the general law for the protection of personal data (lgpd) in brazil: an exploratory survey. In: **2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)**. Las Vegas, NV, USA: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC), 2022. p. 0723–0729. Disponível em: https://ieeexplore.ieee.org/document/9720879. Acesso em: 02 out. 2024.

Fia. **O que é Cibersegurança e Qual a Importância para as Empresas?** 2023. Disponível em: https://fia.com.br/blog/ciberseguranca/. Accessed: 2024-10-02.

Greenwold, S. **Spatial Computing**. 1995. Disponível em: https://acg.media.mit.edu/people/simong/thesis/SpatialComputing.pdf. B.S. Thesis. Acesso em: 22 jan. 2024.

Joshua, J. Information bodies: Computational anxiety in neal stephenson's snow crash. **Interdisciplinary Literary Studies**, Penn State University Press, v. 19, n. 1, p. 17–47, 2017. ISSN 15248429, 2161427X. Disponível em: http://www.jstor.org/stable/10.5325/intelitestud.19.1.0017. Acesso em: 25 out. 2023.

Jota. **Vazamentos de dados no Brasil**. 2022. Disponível em: https://www.jota.info/tributos-e-empresas/mercado/vazamentos-de-dados-no-brasil-28012022#:~:text=5)%20Vazamentos%20de%20dados%20da,consumo%20e%20histÃşrico%20de%20pagamentos.. Acesso em: 28 jun. 2024.

kahneman, D. **Rápido e devagar: duas formas de pensar**: recurso eletrônico. Rio de Janeiro: Objetiva, 2012. 588 p. Disponível em: https://www.objetiva.com.br. Acesso em: 02 out. 2024.

Lobo, L. H. Principais pontos de atenção relacionados a segurança da informação e a proteção de dados pessoais. **Independent Board Member | Comitê de Riscos da Caixa e de Auditoria da BR Partners**, 2023. Acesso em: 23 jul. 2023.

Meta. **Meta Horizon Worlds: Explore Universos Virtuais e Conecte-se com Outros**. 2024. Disponível em: https://www.meta.com/pt-br/experiences/meta-horizon-worlds/2532035600194083/. Acesso em: 02 out. 2024.

Mulholland, C. S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, v. 19, n. 3, p. 159–180, 2018. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1603. Acesso em: 21 mar. 2024.

News, A. **Red Cross Blood Service admits to data breach**. 2016. Disponível em: https://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036?utm_campaign=abc_news_web&utm_content=link&utm_medium=content_shared&utm_source=abc_news_web. Acesso em: 01 out. 2024.

Newzoo, I. **Introducing Newzoo's Intro to the Metaverse Report**. 2021. https://newzoo.com/resources/blog/introducing-newzoos-intro-to-the-metaverse-report. Acesso em: 24 jun. 2023.

Polícia Federal. **Polícia Federal deflagra a Operação Deepwater, que combate a obtenção e vazamento ilegal de dados pessoais de brasileiros pela internet**. 2021. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2021/03/policia-federal-deflagra-a-operacao-deepwater-que-combate-a-obtencao-e-vazamento/-ilegal-de-dados-pessoais-de-brasileiros-pela-internet. Acesso em: 11 jun. 2024.

Radoff, J. **The Metaverse Value Chain**. 2021. https://medium.com/building-the-metaverse/the-metaverse-value-chain-afcf9e09e3a7. Acesso em: 22 jun. 2023.

Roesner, F.; Kohno, T.; Molnar, D. Security and privacy for augmented reality systems. **Communications of the ACM**, v. 57, n. 4, p. 88–96, 2014. Disponível em: https://doi.org/10.1145/2580723.2580730. Acesso em: 03 out. 2024.

Sebastião, M. P. D. A. Proteção aos dados do usuário de serviços digitais pela lgpd e as cláusulas abusivas na política de privacidade. **Cadernos Jurídicos da Faculdade de Direito de Sorocaba**, v. 3, n. 1, p. 107–120, 2022. Disponível em: https://www.fadi.br/revista/index.php/cadernosjuridicos/article/view/92. Acesso em: 2024-06-28.

SEF, U. S. S. de Estado de Fazenda de M. G. **LGPD - lei geral de proteção de dados pessoais - SEF/MG**. 2020. Disponível em: http://www.fazenda.mg.gov.br/transparencia/lgpd/LGPD-SEF-Ciclo-de-Vida-Introducao.pdf. Acesso em: 23 jun. 2024.

SERPRO. **Princípios da LGPD**. 2024. Disponível em: https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/principios-da-lgpd,. Acesso em: 02 out. 2024.

Tecnoblog. **Facebook, Epic Games, Roblox e Microsoft querem um pedaço do metaverso**. 2021. Disponível em: https://tecnoblog.net/noticias/facebook-epic-games-roblox-e-microsoft-querem-um-pedaco-do-metaverso/. Acesso em:02 out. 2024.

UFRJ. **Incidentes de Segurança da Informação**. 2023. Disponível em: https://www.security.ufrj.br/denuncie-um-incidente. Acesso em: 23 jun. 2023.

Vadlamudi, S. The taxonomy of security issues and countermeasures in the metaverse world. In: **2022 International Conference on Recent Trends in Microelectronics, Automation, Computing and Communications Systems (ICMACC)**. Hyderabad, India: IEEE, 2022. p. 553–558. Disponível em: https://ieeexplore.ieee.org/document/10093534. Acesso em: 16 set. 2023.

Vladimirov, I.; Nenova, M.; Nikolova, D.; Terneva, Z. Security and privacy protection obstacles with 3d reconstructed models of people in applications and the metaverse: A survey. In: **2022 57th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)**. Ohrid, North Macedonia: IEEE, 2022. p. 1–4. Disponível em: https://ieeexplore.ieee.org/document/9828791. Acesso em: 02 out. 2024.