



**Centro Universitário de Brasília - CEUB**  
**Faculdade de Ciências Jurídicas e Sociais (FAJS)**  
**Curso de Bacharelado em Direito**

**PEDRO GABRIEL DE SOUZA SILVA**

**DESAFIOS E DIRETRIZES PARA A CONFORMIDADE COM A LGPD EM  
PROJETOS DE REALIDADE AUMENTADA: Uma Análise das Implicações de  
Proteção de Dados.**

**BRASÍLIA - DF**

**2024**

**PEDRO GABRIEL DE SOUZA SILVA**

**DESAFIOS E DIRETRIZES PARA A CONFORMIDADE COM A LGPD EM  
PROJETOS DE REALIDADE AUMENTADA: Uma Análise das Implicações de  
Proteção de Dados.**

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (CEUB)

Orientadora: Professora Rafaela Lisboa Andrade Freitas

**BRASÍLIA - DF**

**2024**

**PEDRO GABRIEL DE SOUZA SILVA**

**DESAFIOS E DIRETRIZES PARA A CONFORMIDADE COM A LGPD EM  
PROJETOS DE REALIDADE AUMENTADA: Uma Análise das Implicações de  
Proteção de Dados**

Artigo científico apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (CEUB)

Orientadora: Professora Rafaela Lisboa Andrade Freitas

**BRASÍLIA - DF, xx de xxxxxx de 2024**

**BANCA AVALIADORA**

---

Professora Orientadora

---

Professor(a) Avaliador(a)

## **RESUMO**

A pesquisa explora os obstáculos e consequências jurídicas da combinação entre a Realidade Aumentada (RA) e a salvaguarda de dados pessoais, concentrando-se na Lei Geral de Proteção de Dados (LGPD). O estudo analisa como a Realidade Aumentada, ao mesclar elementos virtuais com a realidade, recolhe e manipula informações confidenciais de usuários e terceiros, suscitando questões de privacidade e segurança. Para atingir essa meta, foi conduzida uma revisão de literatura de autores renomados e uma análise de casos reais, com o propósito de verificar a aderência das práticas de coleta, processamento e armazenamento de dados em contextos de Realidade Aumentada à LGPD. A pesquisa aponta falhas que podem prejudicar a aplicação efetiva da lei e sugere orientações para assegurar a adesão às regras de proteção de dados. Conclui-se que as entidades enfrentam consideráveis desafios éticos e jurídicos ao empregar essa tecnologia, sendo imprescindível balancear suas vantagens com a salvaguarda dos direitos de privacidade dos cidadãos.

**Palavras-chave:** Realidade aumentada. Proteção de dados. LGPD. Privacidade. Segurança. Legislação.

## **ABSTRACT**

The research explores the legal challenges and implications arising from the intersection of Augmented Reality (AR) and the protection of personal data, with a particular focus on Brazil's General Data Protection Law (LGPD). The study examines how AR, by integrating virtual elements with the real world, collects and processes sensitive information from users and third parties, raising significant concerns about privacy and data security. To achieve this objective, an extensive literature review of distinguished authors was conducted, alongside an analysis of real-world cases, aiming to assess the compliance of data collection, processing, and storage practices within AR environments with the LGPD. The research identifies shortcomings that may hinder the effective enforcement of the law and proposes guidelines to ensure adherence to data protection regulations. The study concludes that entities face substantial ethical and legal challenges when employing this technology, making it essential to balance its advantages with the safeguarding of citizens' privacy rights.

**Key words:** Augmented reality. Data protection. LGPD. Privacy. Security. Legislation.

## SUMÁRIO

<b>INTRODUÇÃO.....</b>	<b>6</b>
<b>1. LEI GERAL DE PROTEÇÃO DE DADOS FRENTE À REALIDADE AUMENTADA.....</b>	<b>9</b>
<b>1.1 Princípios da Proteção de Dados e LGPD.....</b>	<b>10</b>
<b>1.2 Aspectos Legais da Realidade Aumentada.....</b>	<b>13</b>
<b>2. Perspectivas Futuras e Recomendações.....</b>	<b>14</b>
<b>3. CONCLUSÃO.....</b>	<b>20</b>
<b>REFERÊNCIAS.....</b>	<b>22</b>

## INTRODUÇÃO

As profundas mudanças enfrentadas pelas organizações, em decorrência dos avanços tecnológicos modernos, fornecem o contexto primordial para este estudo, que se concentra na interseção entre a realidade aumentada e a proteção de dados pessoais. Diante desse cenário, os objetivos deste trabalho são mais específicos e direcionados, visando examinar os desafios enfrentados pelas organizações ao lidar com a coleta, processamento e armazenamento de dados em ambientes de realidade aumentada. Para tanto, é essencial investigar como a Lei Geral de Proteção de Dados - LGPD se aplica a essas práticas, identificando lacunas e obstáculos que possam comprometer sua implementação eficaz.

Para alcançar tais objetivos, adotou-se uma abordagem metódica e embasada em evidências. Primeiramente, foi realizada uma revisão detalhada da literatura relevante, incluindo obras como "Data Protection: A Practical Guide to UK and EU Law" (CAREY, 2018) e "Proteção de Dados - Contendo narrativas e elementos fundantes" de Bruno Bioni (2021), para compreender profundamente os princípios e regulamentações relacionados à proteção de dados e sua aplicabilidade no contexto da realidade aumentada. Além disso, foram explorados insights oferecidos por autores como Bruce Schneier (2016) em "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World" e Woodrow Hartzog e Evan Selinger (2015) em "Augmented Reality: A Technology and Policy Primer", que abordam questões éticas e políticas na convergência entre tecnologia e privacidade.

Toda pesquisa inicialmente envolve revisão bibliográfica, embora em alguns casos os dados sejam obtidos principalmente de fontes teóricas. A revisão bibliográfica é crucial para fornecer uma compreensão abrangente e crítica do tema em estudo, além de identificar consensos e divergências entre diferentes perspectivas. Serve como base teórica, exigindo uma análise seletiva, analítica e interpretativa de diversas fontes, que devem ser cuidadosamente registradas para referência futura (NASCIMENTO, 2016).

Para embasar a proposta da pesquisa e discorrer os objetivos elencados, no intuito de investigar interdisciplinarmente as implicações legais da utilização da Realidade Aumentada, esta pesquisa é caracterizada como exploratória, cuja metodologia envolve o levantamento bibliográfico. Conforme Rúdio (2012, p. 71), exploratória por estar "interessada em descobrir e observar fenômenos, procurando descrevê-los, classificá-los e interpretá-los". Para Gil (2019), bibliográfica por consistir em utilizar material já publicado como base de informação.

A metodologia confere legitimidade ao discurso científico quando a realidade, que é o problema central da ciência, enquadra-se na descrição natural que aparece aos olhos do

pesquisador (TOMAINO et al. 2016, p. 25). A pesquisa bibliográfica tratará de solucionar um problema ou de angariar conhecimentos empregando informações advindas de materiais gráficos, sonoros e/ou informatizados (BARROS; LEHFELD, 2007, p. 85). Quase todos os estudos requerem esse tipo de trabalho, mas alguns estudos foram desenvolvidos exclusivamente a partir de informações bibliográficas. Parte das pesquisas exploratórias pode ser definida como estudos bibliográficos, bem como certo número de pesquisas realizadas a partir da técnica de análise de conteúdo (GIL, 2019, p. 50-51).

Além disso, a abordagem do estudo é considerada qualitativa, pois ela interpreta os fenômenos e atribui significados durante a pesquisa, sem utilização de estatística. A abordagem é conduzida pela construção de sentidos a partir de processos e variáveis, trabalhando com dados verbais e visuais (BRASILEIRO, 2021).

As bases de dados selecionadas, além dos conceitos explorados das obras clássicas pertinentes ao tema, constituíram em “Scientific Electronic Library Online” (SciELO) e EBSCOhost. Para fixação da amostragem e identificação dos artigos, foram utilizados os descritores, individualmente e combinados, quais sejam, “LGPD”, “realidade aumentada”, “proteção de dados”, “conformidade” e “inovação”. Nesse processo, o operador booleano “E” (AND) foi adotado. O período eleito para escolha das referências consistiu entre os anos de 2018 a 2024.

Em seguida, realizou-se uma análise criteriosa de casos e estudos de pesquisa relacionados, examinando exemplos concretos de como as organizações estão lidando com questões de proteção de dados em projetos de realidade aumentada. Por fim, com base nos insights obtidos, foram propostas diretrizes e recomendações para garantir que os projetos de realidade aumentada estejam em conformidade com os requisitos da LGPD, utilizando contribuições como "Tratamento De Dados Pela Inteligência Artificial" por Marcella Oliveira (2023) e "The Application Of The General Personal Data Protection Law In The Indirect Public Administration: Consent And Data Processing", de Freitas e Rezende (2023).

No mais, e previamente ao que irá ser discutido neste trabalho, é imprescindível entender o que é a Realidade Aumentada - RA, e como funcionam os dispositivos de realidade aumentada. No trabalho “Privacy in an augmented reality” de Andreas Kotsios (2015), o assunto é bastante abordado, no sentido de criar uma cadeia de informações que se estendem do usuário à máquina. Segundo este, a informação que era comunicada por meio de computadores era exposta com a distração criada pela própria máquina, já que o meio, ou seja, o computador, ficava entre a informação e o receptor da informação, ou seja, o usuário do dispositivo.

Nos últimos tempos, com o advento da RA, o espaço entre a informação e o receptor dessa informação tende a diminuir. Ou seja, permite sobrepor elementos virtuais à visão da realidade, literalmente. Um dispositivo capaz de realizar tal feito como, por exemplo, o Apple Vision Pro e Google Glass, pode, tão somente captar e tratar dados sensíveis de terceiros, como também os dados do próprio usuário.

Andreas Kotsios, divide muito bem os três dos principais malefícios que podem ser ocasionados com a realidade aumentada, relatando que, “os usuários de dispositivos de realidade aumentada vestíveis podem realizar três ações que podem resultar em intrusões na privacidade de terceiros, como será esclarecido a seguir. As três ações são: (i) a captura de fotos e vídeos de terceiros; (ii) o carregamento desses registros em espaços privados, semi-públicos ou públicos, como em um site de rede social (SNS) como Facebook, Google+ ou YouTube; e (iii) o processamento do rosto e do corpo dessa pessoa pelo uso de biometria (KOTSIOS, 2015, p. 12).

Assim, este trabalho não apenas analisa os desafios enfrentados pelas organizações na confluência entre realidade aumentada e proteção de dados mas, também, propõe soluções tangíveis e orientações práticas para promover a conformidade com as regulamentações de proteção de dados, especialmente a LGPD, em um contexto de rápida evolução tecnológica. O crescente desenvolvimento da RA em diversos aspectos da vida moderna levanta questões cruciais sobre privacidade e proteção de dados.

A combinação da coleta de dados pessoais em ambientes de RA, principalmente em se tratando de coletas e tratamento de dados, evidencia a necessidade de uniformizar o desenvolvimento com a LGPD, tornando-se um tópico de grande relevância e complexidade. Com sua popularidade em diversas indústrias, como entretenimento, educação, saúde e varejo, destaca-se a urgência de compreender e abordar as implicações de privacidade e proteção de dados com o uso da RA.

A LGPD, como marco regulatório no Brasil, visa garantir a segurança e a privacidade dos dados dos cidadãos, tornando essencial explorar como ela se aplica ao ambiente da realidade aumentada. Nesse contexto, surge a problemática: Como equilibrar as potenciais vantagens da realidade aumentada, como o aprimoramento da experiência do usuário e novas oportunidades de negócios, com as preocupações relacionadas à privacidade e segurança dos dados pessoais coletados, processados e armazenados nesse ambiente?

Desta feita, com o escopo precípua deste trabalho é analisar os desafios da proteção de dados pessoais no contexto da realidade aumentada, com foco na conformidade com a LGPD, esmiuçando os objetivos específicos em (i) investigar as práticas atuais de coleta,



processamento e armazenamento de dados em aplicações de realidade aumentada, (ii) analisar como as disposições da LGPD se aplicam aos dados pessoais coletados em ambientes de realidade aumentada, identificando suas lacunas e desafios e, por fim, (iii) propor diretrizes e recomendações para garantir a conformidade com a LGPD em projetos de realidade aumentada.

Esta pesquisa é de extrema relevância acadêmica devido ao seu potencial para contribuir significativamente para a geração de conhecimento científico em uma área interdisciplinar em rápida evolução. Com o crescente uso da RA em diversos setores há uma lacuna no entendimento abrangente de seus impactos legais. Abordando esse hiato ao explorar os desafios jurídicos e éticos decorrentes da adoção da RA, fornece uma base teórica sólida e insights para futuros trabalhos.

Além disso, as descobertas da pesquisa podem informar a criação de políticas e diretrizes para governos e organizações regulatórias, promovendo um ambiente jurídico mais seguro e transparente para o desenvolvimento e uso da RA. Tem, portanto, o potencial de beneficiar a sociedade em geral, fornecendo uma compreensão mais ampla e informada das implicações legais da RA, e ao abordar preocupações como privacidade, segurança e conformidade legal, a pesquisa visa, não somente proteger os direitos individuais dos cidadãos e promover uma adoção responsável e ética da tecnologia, mas também auxiliar na criação de um ambiente colaborativo para as bigtechs se desenvolverem em um âmbito de segurança aos usuários.

Além disso, ao identificar áreas de risco e possíveis lacunas na legislação existente, a pesquisa pode informar o debate público e influenciar a formulação de políticas para garantir que a RA seja utilizada de maneira benéfica e ética para toda a sociedade, esperando-se contribuir para uma melhor compreensão das questões de privacidade e de proteção de dados na RA.

## **1. LEI GERAL DE PROTEÇÃO DE DADOS FRENTE À REALIDADE AUMENTADA**

Primordialmente, ao estar diretamente vinculado aos seus dados pessoais, capturando gestos, preferências, interesses e diversas facetas do comportamento, é evidente que essa tecnologia enfrenta desafios em relação às legislações de privacidade. A LGPD estabelece princípios fundamentais para garantir que o tratamento de dados seja realizado de forma ética e legal. Conforme se extrai do texto “Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados”, de Laura Schertel Mendes e Danilo Doneda (2018), esses princípios incluem a finalidade, que exige o uso dos dados para propósitos específicos e legítimos; a adequação,

que assegura a compatibilidade do tratamento com as finalidades informadas; e a necessidade, que limita o tratamento ao mínimo essencial para atingir seus objetivos.

A integração da RA com a LGPD apresenta desafios significativos, especialmente no que se refere à privacidade e segurança. A RA, por sua natureza, requer a coleta de grandes quantidades de dados pessoais, como localização e imagens. Garantir a conformidade com a LGPD exige que as empresas obtenham consentimento explícito dos usuários e adotem medidas robustas de segurança, o que pode ser complexo e oneroso. Apesar desses desafios, essa integração também oferece oportunidades valiosas. A conformidade com a LGPD pode impulsionar a inovação responsável, levando ao desenvolvimento de soluções de RA que respeitem a privacidade dos usuários desde a concepção, fortalecendo a confiança dos consumidores e abrindo novos mercados, especialmente em áreas sensíveis como saúde e educação, onde a proteção de dados é crucial. representando um equilíbrio entre os desafios de proteger a privacidade e as oportunidades de criar soluções inovadoras que atendam às exigências legais.

### **1.1 Princípios da Proteção de Dados e LGPD**

Antes de nos aprofundarmos no cerne principal deste trabalho, qual seja, a Proteção de Dados e LGPD com o Advento da Realidade Aumentada, é importante entendermos os princípios que orientam o tratamento de dados pessoais. Como o renomado Professor Marcio Pestana, “(...)conhecer princípios equivale a conhecer a essência da matéria sob atenção, facilitando, sobremaneira, a dissecação do objeto sob estudo. Desconhecer os princípios, ao reverso, é caminhar tateantemente por entre disposições e preceptivos, sem visão de largueza e amplitude, prejudicando, com tons de definitividade, a possibilidade que se encerra de investigar-se e aprofundadamente conhecer-se o objeto” (PESTANA, 2019, p. 2).

A LGPD concede aos titulares de dados o direito de exigir informações sobre o tratamento de seus dados, incluindo a identificação das pessoas e a forma como foram tratados. Além disso, os titulares têm o direito de se opor ao uso de seus dados e à finalidade para a qual foram tratados. Nesta senda, no artigo 6º da LGPD (BRASIL, 2018), foram estabelecidos os principais requisitos a serem observados nas atividades envolvendo o tratamento de dados pessoais, abordados nos parágrafos que seguem, dentre elas a realidade aumentada, fundamentais para garantir que o tratamento dos dados seja realizado de forma ética e legal.

O primeiro princípio é o da finalidade, que exige que o tratamento dos dados seja feito para propósitos legítimos, específicos e informados ao titular dos dados, sem possibilidade de

uso posterior incompatível com essas finalidades. Isso significa que os dados devem ser utilizados de forma sensata e transparente, respeitando a vontade do titular. Por sua vez, o princípio da adequação refere-se à compatibilidade do tratamento com as finalidades informadas ao titular, levando em consideração o contexto do tratamento. Isso implica em estabelecer uma relação lógica entre o tratamento e a finalidade objetivada, garantindo que os dados sejam utilizados de maneira pertinente e adequada (DONEDA, 2024).

Para limitar o tratamento ao mínimo necessário para alcançar suas finalidades, utilizando apenas os dados pertinentes, proporcionais e não excessivos, o princípio da necessidade traduz que apenas os dados essenciais devem ser tratados, evitando qualquer forma de excesso ou abuso. O princípio do livre acesso garante aos titulares dos dados o direito de consultar de forma facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Isso garante que os titulares possam acessar e conhecer seus dados após o tratamento (BRASIL, 2018).

O princípio da qualidade dos dados assegura a exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Isso significa que os dados devem ser precisos, claros e relevantes para a finalidade específica do tratamento. A transparência é outro princípio fundamental, que garante aos titulares dos dados informações claras, precisas e facilmente acessíveis sobre o tratamento realizado e os respectivos agentes de tratamento. Isso permite que os titulares compreendam o que está acontecendo com seus dados e quem está envolvido no processo.

O princípio da segurança exige que os protagonistas do tratamento utilizem medidas técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. Isso garante a segurança e a confidencialidade dos dados durante todo o processo de tratamento (BRASIL, 2018).

A prevenção é um princípio que destaca a importância de adotar medidas para evitar danos em virtude do tratamento de dados pessoais. Isso significa que é necessário prevenir qualquer forma de dano ou violação dos dados, garantindo a integridade e a segurança das informações. O princípio da não discriminação proíbe o tratamento dos dados para fins discriminatórios ilícitos ou abusivos. Isso significa que os dados não devem ser utilizados de forma discriminatória ou injusta, respeitando os direitos e a dignidade dos titulares (DONEDA, 2021).

Por fim, o princípio da responsabilização e da prestação de contas exige que os agentes responsáveis pelo tratamento demonstrem a adoção de medidas eficazes para cumprir as

normas de proteção de dados e garantir a eficácia dessas medidas. Isso inclui a responsabilidade de comprovar que os procedimentos foram seguidos corretamente e que os dados foram tratados de acordo com a lei (BRASIL, 2018).

A Lei Geral de Proteção de Dados (LGPD) desempenha um papel fundamental na regulamentação e fiscalização do tratamento de dados pela Realidade Aumentada (RA). O artigo 18 da LGPD estabelece uma série de direitos para os titulares de dados em relação ao tratamento de seus dados por sistemas de Realidade Aumentada, do titular dos dados pessoais em relação ao controlador que os trata. Esses direitos refletem um avanço significativo na proteção da privacidade e dos dados pessoais dos cidadãos brasileiros, alinhando o país às melhores práticas internacionais nesse campo.

Primeiramente, o artigo assegura ao titular o direito à confirmação da existência de tratamento de seus dados pessoais, garantindo transparência e controle sobre suas informações. Além disso, o titular tem o direito de acessar seus dados, o que é essencial para que possa verificar a veracidade e a exatidão das informações que estão sendo processadas.

Outro ponto importante é a possibilidade de correção de dados incompletos, inexatos ou desatualizados, o que contribui para a manutenção da precisão e integridade das informações pessoais. O artigo prevê a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação, promovendo uma maior adequação e minimização dos dados pessoais tratados (DONEDA, 2021).

A portabilidade dos dados a outro fornecedor de serviço ou produto é um direito essencial, que permite ao titular a livre movimentação de suas informações, promovendo a concorrência e a liberdade de escolha. Isso é especialmente relevante em um contexto de economia digital, onde a mobilidade dos dados é crucial para a dinâmica do mercado. Além disso, o artigo 18 estabelece a possibilidade de eliminação dos dados pessoais tratados com o consentimento do titular, salvo em situações específicas previstas na legislação, o que reforça o princípio da autodeterminação informativa.

Outros direitos contemplados pelo artigo incluem a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, bem como a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências dessa negativa. Esses aspectos contribuem para uma maior transparência e conscientização do titular sobre o tratamento de seus dados pessoais.

Os titulares têm o direito de obter do controlador de Realidade Aumentada a confirmação de que seus dados estão sendo tratados, bem como o acesso a esses dados. Além disso, os titulares têm o direito de corrigir, atualizar ou complementar seus dados, e de

solicitar a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a legislação.

Esses direitos conferem aos titulares um maior controle sobre seus dados pessoais, garantindo que possam verificar como estão sendo utilizados pela Realidade Aumentada e tomar medidas para corrigir qualquer informação imprecisa ou inadequada. Isso promove a transparência e a responsabilidade no tratamento de dados pela Realidade Aumentada, contribuindo para proteger a privacidade e os direitos dos usuários.

## **1.2 Aspectos Legais da Realidade Aumentada**

Passando a entender um pouco sobre os princípios que norteiam a LGPD, é possível analisar como a utilização da Realidade Aumentada (RA) pode apresentar uma série de implicações legais que precisam ser cuidadosamente consideradas, especialmente no que diz respeito à privacidade, segurança e conformidade com a legislação de proteção de dados.

Em primeiro lugar, as questões de privacidade são um ponto crucial. Dispositivos de RA têm a capacidade de capturar imagens e vídeos do ambiente circundante de forma discreta, o que levanta preocupações sobre a invasão da privacidade das pessoas que estão sendo gravadas sem o seu consentimento. É imperioso destacar que a captura de imagens e vídeos pode comprometer a privacidade de comportamento e ação dessas pessoas, uma vez que elas podem se sentir constantemente monitoradas e ajustar seu comportamento em resposta a essa vigilância percebida.

Além disso, a utilização de biometria, como o reconhecimento facial, em aplicativos de RA pode representar uma séria ameaça à privacidade dos indivíduos. Por exemplo, reconhecimento facial pode extrair informações sensíveis sobre uma pessoa, como sua identidade, seu consentimento explícito, sem sua autorização. Isso levanta questões sobre o controle e a propriedade dos dados biométricos e como eles são armazenados, processados e compartilhados.

Em termos de segurança, a utilização de dispositivos de RA também pode representar riscos significativos. Por exemplo, a dependência de dispositivos de RA para fornecer informações em tempo real pode expor os usuários a ameaças cibernéticas, como ataques de *phishing* ou *malware*. Além disso, a integração de informações virtuais com o ambiente físico pode criar novos pontos de vulnerabilidade que podem ser explorados por hackers ou malfeitores.

Para Rosas (2023), em seu livro *Inteligência Artificial - Regulação ética a partir das regras de Proteção dos Dados Pessoais*, a arquitetura original do ciberespaço nasceu na forma de um modelo, que não comportava regulação ou monitoramentos externos. A partir desse apontamento, que vem muito antes da própria criação de RA, determina que, sem uma regulamentação, ou diretrizes bem estabelecidas, a tecnologia não obedecerá direitos básicos e principiológicos da LGPD.

Quanto à conformidade com a legislação de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil ou o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia (EUROPA, 2016), as empresas que desenvolvem e utilizam tecnologias de RA devem garantir que estão em conformidade com os requisitos legais de coleta, armazenamento, processamento e compartilhamento de dados pessoais. Isso inclui a obtenção de consentimento válido dos usuários para coletar e utilizar seus dados, bem como implementar medidas de segurança adequadas para proteger esses dados contra acessos não autorizados ou violações de segurança.

Em suma, a utilização da Realidade Aumentada apresenta uma série de implicações legais, incluindo questões de privacidade, segurança e conformidade com a legislação de proteção de dados. Para mitigar esses riscos, é essencial que as empresas que desenvolvem e utilizam tecnologias de RA adotem uma abordagem proativa para garantir que estão em conformidade com as leis e regulamentos aplicáveis e proteger os direitos e privacidade dos usuários.

## **2. Perspectivas Futuras e Recomendações**

A Constituição tem como uma de suas principais funções a defesa de direitos, garantias e liberdades fundamentais individuais. Estes direitos, por sua vez, estão intrinsecamente relacionados ao desenvolvimento tecnológico e frequentemente são impactados pelas diversas aplicações das novas tecnologias. Como destaca a autora Eduarda Moraes Chacon Rosas, os algoritmos, em particular, atualmente não são apenas adjetivo de definição da sociedade (sociedade algorítmica, sociedade de dados), como também impactam de modo relevante diversos aspectos da vida do cidadão, desde sua autoestima até questões de saúde, emprego, relacionamento interpessoal, habitação, finanças etc (ROSAS, 2023).

Nesse contexto, a integração da Realidade Aumentada (RA) com a Lei Geral de Proteção de Dados (LGPD) traz uma série de desafios e oportunidades que são cruciais para o desenvolvimento ético e legal dessa tecnologia emergente. À medida que a RA se torna mais presente em setores como educação, entretenimento e saúde, as questões de privacidade e

segurança dos dados dos usuários ganham cada vez mais relevância. A conformidade com a LGPD, portanto, não é apenas uma exigência legal, mas também um elemento essencial para a construção de confiança entre empresas e consumidores.

No entanto, a natureza interativa e invasiva da Realidade Aumentada (RA) apresenta desafios únicos na coleta, tratamento e proteção de dados pessoais, que precisam ser enfrentados com estratégias inovadoras e rigorosas. Neste contexto, é fundamental discutir os principais obstáculos e as possíveis soluções para garantir que a aplicação da RA seja não apenas tecnicamente avançada, mas também legalmente conforme e eticamente responsável.

Diversos mecanismos tecnológicos estão sendo utilizados para influenciar, manipular ou intervir diretamente na vida humana. Por essa razão, a tecnologia tem se tornado objeto central de debate ético e indagação moral, sendo que “as implicações de direito, inclusive de índole constitucional, são uma consequência inevitável do momento histórico vivido” (ROSAS, 2023, p.126).

Para a autora, exemplos como os sistemas de escore levantam importantes questões: “como direitos fundamentais, como a dignidade humana, podem ser preservados em um contexto de categorização automática de pessoas? O que esperar da privacidade e da preservação do valor individual dos avaliados? Além disso, como garantir a proteção aos dados pessoais processados freneticamente para atender a interesses corporativos e governamentais, muitas vezes em detrimento do bem-estar e consentimento dos titulares?” (ROSAS, 2023, p.126).

Ao aplicar a RA em conformidade com a LGPD, surgem desafios específicos, como a coleta excessiva de dados e os riscos à privacidade dos usuários. A RA frequentemente envolve a captura de informações sensíveis, como localização, imagens e interações dos usuários. Para estar em conformidade com a LGPD, é necessário que as empresas obtenham o consentimento explícito dos usuários, além de garantir que esses dados sejam tratados de forma segura e transparente.

A identificação e categorização correta dos dados coletados como sensíveis, de acordo com a LGPD, é crucial para evitar violações. A RA, com sua capacidade de sobrepor informações digitais ao mundo real, já está amplamente inserida em áreas como educação, entretenimento, saúde e varejo. No entanto, essa integração traz à tona questões complexas sobre privacidade, segurança e conformidade com a LGPD, exigindo uma abordagem cuidadosa e estratégica.

Um dos principais desafios nessa integração é a coleta e tratamento de dados pessoais. A RA, por sua natureza interativa, demanda o acesso a uma vasta quantidade de informações

dos usuários, como localização, imagens e dados de comportamento. Sob a ótica da LGPD, essas práticas precisam ser rigorosamente controladas, com consentimento explícito e informado dos usuários. Esse requisito pode ser difícil de atender, uma vez que muitos usuários não compreendem plenamente as implicações de compartilhar seus dados em ambientes de RA. Além disso, o desafio de anonimizar esses dados, sem comprometer a funcionalidade dos aplicativos, é significativo, considerando que a personalização é um dos pilares da experiência em RA.

Outro ponto crítico a ser considerado na integração da Realidade Aumentada (RA) com a Lei Geral de Proteção de Dados (LGPD) é a segurança dos dados. Com o aumento da utilização da RA, os riscos de ataques cibernéticos e vazamentos de informações se tornam mais acentuados. A LGPD exige que as empresas adotem medidas de segurança robustas para proteger os dados dos usuários. No entanto, implementar essas medidas em sistemas de RA, que frequentemente operam em tempo real e em diversos dispositivos, é uma tarefa complexa. Qualquer falha nesse aspecto pode resultar não apenas em penalidades severas, mas também em danos irreparáveis à reputação das empresas envolvidas.

Um estudo relevante sobre a questão da coleta de dados e a utilização de algoritmos é o artigo "Gestão de algoritmos pelas plataformas de redes sociais online - uma análise dos termos de uso do Facebook e sua interface com a ética", escrito pela Dra. Regina Rossetti e pela Mestre Kethly Garcia. O artigo explora o documento "Políticas de Privacidade" da Meta, empresa responsável pelo Facebook e Instagram, destacando a complexa relação entre a coleta de dados e os algoritmos. A empresa menciona o uso de "sistemas" seis vezes, cinco das quais estão diretamente relacionadas ao tratamento automatizado de dados. Esses sistemas desempenham um papel crucial na personalização da experiência dos usuários, processando informações automaticamente para definir perfis e direcionar conteúdos específicos.

Embora a personalização tenha seus benefícios, como Rossetti e Garcia (2024) enfatizam, ela também levanta preocupações significativas sobre privacidade e o poder que as empresas exercem ao modelar comportamentos com fins comerciais. O processamento de dados, como destacado no artigo, é majoritariamente voltado para a otimização de anúncios e a criação de perfis de usuários, com uma combinação de automação e intervenção humana.

Apesar dos desafios mencionados, a integração da RA com a LGPD abre oportunidades para o desenvolvimento de soluções inovadoras que atendam aos requisitos legais de proteção de dados. A conformidade com a LGPD pode ser vista como um catalisador para a inovação responsável. Empresas que adotam a abordagem de "Privacy by Design" — na qual a privacidade é integrada desde a concepção do produto (MARRAFON,



2020) — não apenas cumprem a legislação, mas também têm a oportunidade de se destacar no mercado, conquistando a confiança dos consumidores e criando um diferencial competitivo. Essa abordagem pode levar ao desenvolvimento de soluções de RA mais seguras e centradas no usuário, que respeitam a privacidade e a proteção de dados desde o início do processo de design.

No entanto, não há uma fórmula que resolva esses problemas de maneira definitiva, especialmente diante da falta de estrutura estatal para uma fiscalização eficaz. Ainda assim, o desenvolvimento e a aplicação de tecnologias como a Inteligência Artificial (IA) e a (RA) não ocorrem em um vácuo regulatório. Na área de proteção de dados, já existem normas constitucionais e infraconstitucionais que estabelecem direitos e deveres claros sobre como proceder – ou não proceder.

O direito à proteção de dados, por exemplo, foi elevado ao status de direito fundamental com a promulgação da Emenda Constitucional n.º 115, em 11 de fevereiro de 2022, que adicionou o inciso LXXIX ao artigo 5º da Constituição Federal (BRASIL, 1988). Além disso, a LGPD, como já amplamente discutido em tópicos anteriores, exige transparência e comunicação clara, o que oferece uma oportunidade para educar os usuários sobre a importância da privacidade.

Aplicativos de RA que conseguirem transmitir de maneira acessível como os dados são coletados e utilizados poderão fortalecer a relação de confiança com seus usuários – algo essencial em um mercado cada vez mais atento às questões de privacidade, essa integração entre a também pode estimular a criação de novos mercados, especialmente em setores sensíveis como saúde e educação, onde a proteção de dados é crucial. Empresas que oferecem soluções de RA em conformidade com a LGPD poderão explorar nichos de mercado que valorizam a segurança e a privacidade, ampliando suas oportunidades de negócio.

Do ponto de vista jurídico, bases como o consentimento, o cumprimento de obrigação legal e o legítimo interesse permitem que as organizações tratem dados de maneira legítima. No entanto, a escolha da base legal adequada requer uma análise criteriosa do contexto específico do tratamento de dados, algo que muitas empresas ainda têm dificuldade em realizar, dada a pouca familiaridade com a legislação.

A transparência no tratamento de dados é outro aspecto crucial da LGPD. Como argumenta Márcio Pestana, em “Os princípios no tratamento de dados LGPD” (PESTANA, 2019), a transparência é essencial para que os titulares dos dados possam exercer plenamente seus direitos, como o acesso, correção ou exclusão de suas informações pessoais. Para garantir essa transparência, as empresas devem adotar uma postura proativa, oferecendo

clareza sobre as finalidades da coleta, os métodos de tratamento e um canal de comunicação eficaz. Ao fazer isso, não apenas fortalecem a confiança com os consumidores, mas também garantem que suas práticas estejam em conformidade com os princípios da legislação.

Para Frazão (2019), a economia digital centrada nos dados vem trazendo transformações em ritmo acelerado, muitas vezes sem as reflexões jurídicas e éticas necessárias. Parte dessa dificuldade deve-se à assimetria informacional. Com efeito, na economia movida a dados, os algoritmos constituem verdadeiras caixas pretas, pois ninguém sabe ao certo como funciona esse poder de ação e de predição. Evidente que a transparência é fundamental para o bom desenvolvimento da RA.

Além da transparência, a segurança dos dados pessoais tratados pelas empresas é uma preocupação central da LGPD. Um dos pontos importantes para a adequação à LGPD é a contratação de um Data Protection Officer (DPO). Conforme se extrai de Doneda (2021), o DPO é uma figura central para assegurar que a empresa esteja em conformidade com as regras de proteção de dados. Este profissional tem a responsabilidade de intermediar a relação entre a organização, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Contudo, para muitas empresas, especialmente as de menor porte, a contratação de um DPO interno pode ser custosa, levando à busca por alternativas, como a terceirização dessa função.

Os Relatórios de Impacto à Proteção de Dados (RIPD) também constituem uma ferramenta essencial para mapear e mitigar riscos no tratamento de dados. Esses relatórios devem descrever as operações de tratamento de dados, identificar os riscos associados e delinear as medidas de segurança adotadas. Segundo a própria ANPD, essa documentação pode ser solicitada a qualquer momento, principalmente no caso de tratamento de dados sensíveis, tornando-se, portanto, fundamental para uma boa governança de dados.

A proteção de dados pessoais envolve uma gama de aspectos técnicos, econômicos, jurídicos, além de questões relacionadas à circulação e armazenamento de dados na internet e modelos globais de negócio. Trata-se de um tema transdisciplinar vinculado à governança da internet – e, mais especificamente, à governança de dados – que envolve a proteção efetiva dos direitos humanos, como o livre desenvolvimento da personalidade, a autodeterminação informativa e a proteção da privacidade. Também é importante considerar o desenvolvimento econômico, a segurança jurídica e a inovação.

Diante desse cenário, a adequação à LGPD não é apenas uma questão de cumprimento legal, mas também uma oportunidade para as empresas revisarem suas práticas de coleta e tratamento de dados. Esse processo pode aprimorar a relação com seus clientes e posicionar as organizações de maneira ética e responsável no mercado. A conformidade com a lei deve ser

vista como um investimento na credibilidade e na segurança da empresa, além de uma proteção contra possíveis sanções e danos à reputação.

A integração da Realidade Aumentada (RA) no ambiente digital representa uma inovação significativa, oferecendo inúmeras vantagens, como o aprimoramento da experiência do usuário e a criação de novas oportunidades de negócios. Entretanto, essa evolução tecnológica traz à tona preocupações cruciais relacionadas à privacidade e segurança dos dados pessoais, exigindo um equilíbrio delicado entre a exploração das potencialidades da RA e a proteção dos direitos dos usuários. Para garantir esse equilíbrio, é necessário implementar uma abordagem estratégica que considere tanto os benefícios quanto os riscos associados à coleta e ao processamento de dados.

Primeiramente, a transparência no uso de dados é fundamental para construir confiança entre as empresas que utilizam RA e os usuários. Em segundo lugar, as empresas devem adotar medidas rigorosas de segurança da informação para proteger os dados coletados durante as interações com a RA, enfatiza-se, portanto a importância de implementar práticas robustas de proteção de dados, como criptografia e controle de acesso, para salvaguardar as informações pessoais dos usuários. Além disso, é imprescindível que haja um protocolo claro para o tratamento de incidentes de segurança, incluindo a notificação imediata da ANPD em caso de vazamentos.

Essas práticas não apenas mitigam os riscos associados ao uso da RA, mas também reforçam a imagem da empresa como uma entidade responsável e comprometida com a privacidade dos usuários. Outro aspecto importante para equilibrar os benefícios da RA e a proteção de dados é a definição clara das bases legais para a coleta de informações. A LGPD estabelece que o tratamento de dados deve ser justificado por uma base legal adequada, como consentimento ou legítimo interesse.

Por fim, a formação de um Data Protection Officer (DPO) ou a terceirização dessa função pode ser uma estratégia eficaz para garantir a conformidade com a LGPD e, simultaneamente, fomentar a inovação em RA. O DPO atua como um intermediário entre a empresa, os usuários e a ANPD, sendo responsável por garantir que as práticas de tratamento de dados estejam em conformidade com a legislação vigente. Essa função é especialmente relevante em um ambiente de tecnologia em rápida evolução, onde as normas e regulamentos podem mudar rapidamente.

Em síntese, equilibrar as vantagens da realidade aumentada com as preocupações relacionadas à privacidade e segurança dos dados pessoais exige uma abordagem multifacetada que envolva transparência, segurança, fundamentação legal e governança de

dados. Ao adotar práticas responsáveis e éticas, as empresas podem aproveitar as oportunidades que a RA oferece, ao mesmo tempo em que protegem os direitos dos usuários e cumprem as exigências legais. Esse equilíbrio é essencial para garantir que a inovação tecnológica ocorra de maneira sustentável e respeitosa, promovendo uma relação de confiança entre empresas e consumidores.

### **3. CONCLUSÃO**

O estudo realizado sobre a interseção entre a Realidade Aumentada (RA) e a Lei Geral de Proteção de Dados (LGPD) permitiu identificar um cenário complexo que demanda tanto inovação quanto responsabilidade das organizações, alcançando os objetivos traçados outrora neste artigo. A RA, ao proporcionar experiências imersivas e enriquecedoras para os usuários, levanta também desafios significativos no que tange à proteção dos dados pessoais. Esta tecnologia exige a coleta, o processamento e o armazenamento de grandes quantidades de informações sensíveis, o que coloca as empresas diante de um dilema: Como equilibrar as potenciais vantagens da realidade aumentada, como o aprimoramento da experiência do usuário e novas oportunidades de negócios, com as preocupações relacionadas à privacidade e segurança dos dados pessoais coletados, processados e armazenados nesse ambiente?

Um dos pontos centrais para alcançar esse equilíbrio reside no respeito às exigências impostas pela LGPD, que busca garantir a proteção dos dados pessoais em um ambiente cada vez mais digital. A legislação impõe a necessidade de adoção de medidas de segurança robustas e de transparência na comunicação com os titulares dos dados, além de fomentar práticas que assegurem a integridade e o controle das informações coletadas. Para as empresas que desejam explorar as potencialidades da RA, é essencial compreender que a conformidade com a lei não é apenas uma obrigação legal, mas também uma oportunidade de fortalecer a confiança do consumidor e de consolidar sua posição de mercado.

Conforme abordado por Ronaldo Lemos, colunista semanal da Folha de São Paulo, Advogado, especialista em tecnologia reconhecido internacionalmente, a transparência no uso de dados pessoais é um princípio fundamental para garantir o direito de privacidade dos usuários. No contexto da RA, essa transparência deve ser priorizada para que os usuários compreendam claramente o que está sendo coletado, por que está sendo coletado e como suas informações serão tratadas. Isso requer a criação de políticas de privacidade acessíveis e compreensíveis, que venham detalhar as finalidades da coleta de dados e os procedimentos envolvidos no tratamento dessas informações. As empresas que forem capazes de promover

um diálogo claro e transparente com seus usuários estarão não apenas cumprindo as exigências da LGPD, mas também demonstrando um compromisso ético com a proteção de dados.

Outro aspecto crucial é a adoção de medidas de segurança adequadas para a proteção dos dados pessoais. A RA depende de uma ampla coleta de informações sobre os usuários, muitas vezes incluindo dados sensíveis, como localização geográfica, comportamentos e preferências. Marco Marrafon, em suas discussões sobre Direito Digital, enfatiza que a proteção desses dados deve ser garantida por meio de mecanismos como a criptografia e a implementação de políticas de segurança cibernética. Além disso, é imprescindível que as organizações realizem auditorias frequentes e mantenham registros claros de todas as operações realizadas com os dados. Em caso de incidentes de segurança, como vazamento de informações, a notificação imediata à Autoridade Nacional de Proteção de Dados (ANPD) é essencial para garantir a transparência e a responsabilização da empresa.

Nesse contexto, o papel do Data Protection Officer (DPO) ou Encarregado de Dados Pessoais é cada vez mais relevante. A função do DPO, prevista na LGPD, é essencial para garantir a gestão adequada dos dados pessoais dentro das organizações. A nomeação de um DPO ou a contratação de um serviço terceirizado de proteção de dados oferece às empresas uma forma eficaz de garantir a conformidade contínua com a legislação. O DPO atua como um elo entre a empresa, os titulares dos dados e a ANPD, sendo responsável por monitorar as operações de tratamento de dados e garantir que estas estejam de acordo com as bases legais estabelecidas pela LGPD.

Para equilibrar as vantagens comerciais e tecnológicas da RA com as exigências da proteção de dados, as empresas também devem analisar cuidadosamente as bases legais que fundamentam o tratamento de informações pessoais. Segundo a LGPD, o tratamento de dados deve ser sempre justificado por uma base legal adequada, como o consentimento do titular ou o legítimo interesse da empresa. Onde, conforme amplamente discutido neste trabalho, uma análise detalhada e criteriosa dessas bases legais é essencial para assegurar que a coleta e o uso de dados em ambientes de RA sejam legítimos e transparentes. Quando a coleta de dados é fundamentada por bases legais adequadas, as empresas podem explorar as vantagens da RA com mais segurança jurídica e ética.

Adicionalmente, o uso de relatórios de impacto à proteção de dados surge como uma prática recomendada pela LGPD para garantir que as empresas tenham controle sobre as operações realizadas com os dados pessoais e que avaliem os riscos potenciais associados à RA. Esses relatórios, como mencionados na legislação, permitem às empresas mapear todas

as operações realizadas com dados pessoais, identificar os principais riscos e implementar medidas de segurança adequadas para mitigá-los. A ANPD pode solicitar esses documentos a qualquer momento, especialmente em casos de tratamento de dados sensíveis ou quando o tratamento é justificado pelo legítimo interesse da empresa. Logo, a elaboração de relatórios de impacto é uma ferramenta essencial para assegurar a conformidade com a LGPD e para garantir que a inovação tecnológica proporcionada pela RA não ocorra em detrimento dos direitos dos usuários.

Percebeu-se, ao responder o problema de pesquisa traçado, que o equilíbrio entre as vantagens da realidade aumentada e a proteção dos dados pessoais, portanto, requer uma abordagem integrada, que inclua não apenas a conformidade com a legislação vigente, mas também uma visão estratégica e ética sobre a inovação digital. Ao adotar medidas de segurança robustas, promover a transparência e garantir o controle efetivo sobre o tratamento de dados, as empresas estarão posicionadas para explorar as oportunidades oferecidas pela RA de maneira sustentável. Ao mesmo tempo, essas práticas permitirão às organizações respeitar os direitos de privacidade dos usuários, contribuindo para o desenvolvimento de um ambiente digital mais seguro e confiável.

Conclui-se que a integração da Realidade Aumentada com a LGPD é um desafio inevitável, mas também uma oportunidade única para as empresas que souberem navegar por essa complexa interseção entre inovação e responsabilidade. Ao garantir o equilíbrio adequado entre o uso de tecnologias avançadas e a proteção dos dados pessoais, as organizações estarão preparadas para se destacar em um mercado digital em rápida evolução, ao mesmo tempo em que asseguram a confiança e a segurança de seus clientes.

## REFERÊNCIAS

BARROS, A. J. S. B.; LEHFELD, N. A. S. **Fundamentos de metodologia científica**. 3. ed. São Paulo: Pearson Prentice Hall, 2007.

BIONI, Bruno. **Proteção de Dados**: Contendo narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em 2 set. 2024.

BRASIL. **Lei nº 13.709 de 14/08/2018**, publicada no Diário Oficial da União (D.O.U.).

Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/Lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm)  
Acesso em: 24 abr. 2024.

BRASILEIRO, A. M. M. **Como produzir textos acadêmicos e científicos**. São Paulo: Contexto, 2021.

CAREY, Peter. **Data Protection - A practical Guide to UK and EU Law**. 5º ed. United States of America by Oxford University: Oxford University Press, 2018.

DONEDA, Danilo. **Da Privacidade À Proteção De Dados Pessoais - 3ª Edição**, 2021.

EUROPA. Parlamento Europeu; Conselho Europeu. **Regulamento (UE) 2016/679 de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE** (Regulamento Geral sobre a Proteção de Dados). 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434>. Acesso em 9 set. 2024.

FRAZÃO, Ana. Plataformas digitais, Big Data e riscos para os direitos de personalidade. In: TEPEDINO, Gustavo. MENEZES, Joyciane Bezerra (coords). **Autonomia privada, liberdade existencial e direitos fundamentais**. Belo Horizonte: Fórum, 2019, p. 341.

FREITAS, Cinthia Obladen de Almeida; REZENDE, Laura Wihby. The application of the General Personal Data Protection Law in the indirect public administration: consent and data processing. **Lex Humana**, v. 15, n. 4, p. [números de páginas], 2023. ISSN 2175-0947. Copyright © Universidade Católica de Petrópolis, Rio de Janeiro, Brasil.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo, SP: Atlas, 2019.

HARTZOG, Woodrow; SELINGER, Evan. **Augmented Reality: A Technology and Policy Primer**. 2015.

KOTSIOS, Andreas. Privacy in an augmented reality. **International Journal of Law and Information Technology**, Volume 23, Issue 2, Summer 2015, Pages 157–185. DOI: <https://doi.org/10.1093/ijlit/eav003>. Published: 21 March 2015.

LEMOS, Ronaldo. **Direito na era digital: Aspectos negociais, processuais e registraes**. Editora JusPodivm. 2022.

LIMA, T. C. S.; MIOTO, R. C. T. **Procedimentos metodológicos na construção do conhecimento científico: a pesquisa bibliográfica**. Revista Katál. 10(esp.). 37-45, 2007.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Técnicas de pesquisa (digital)**. 9. ed. São Paulo: Atlas, 2021.

MARRAFON, Marco Aurélio; COUTINHO, Luiza Leite Cabral Loureiro. Princípio da privacidade por design: fundamentos e efetividade regulatória na garantia do direito à proteção de dados. **Revista Eletrônica Direito e Política, Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI**, Itajaí, v.15, n.3, 3º quadrimestre de 2020.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 120, p. 474, 2018.

NASCIMENTO, Francisco Paulo do. Classificação da Pesquisa. Natureza, método ou abordagem metodológica, objetivos e procedimentos. In: \_\_\_\_\_. **Metodologia da Pesquisa Científica: teoria e prática – como elaborar TCC**. Brasília: Thesaurus, 2016.

OLIVEIRA, Marcella Vaz Guimarães De. Tratamento De Dados Pela Inteligência Artificial Data Processing By Artificial Intelligence Tratamiento De Datos Mediante Inteligência Artificial. **Revista Foco**. Curitiba (PR). v.16. n.8. p.01-10. 2023

PEROVANO, Dalton Gean. **Manual de metodologia da pesquisa científica** (digital). Curitiba: InterSaberes, 2016.

PESTANA, Marcio. Os princípios no tratamento de dados LGPD. **Conjur**, 10 de julho de 2019. Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestanalgpd.pdf> Acesso em: 25 abr. 2024.

ROSAS, Eduarda Moraes Chacon. **Inteligência artificial: regulação ética a partir das regras de proteção dos dados pessoais**. Rio de Janeiro: GZ, 2023.

ROSSETTI, Regina; GARCIA, Kethly. Gestão de algoritmos pelas plataformas de redes sociais online: uma análise dos termos de uso do Facebook e sua interface com a ética. **P2P & Inovação**, Rio de Janeiro, v. 11, n. 1, p. 1-17, jul./dez. 2024.

RÚDIO, F. V. **Introdução ao projeto de pesquisa científica**. 26. ed. Petrópolis: Vozes, 2012.

SÁ-SILVA, J. R.; ALMEIDA, C. D.; GUINDANI, J. F. **Pesquisa documental: pistas teóricas e metodológicas**. Revista Brasileira de História & Ciências Sociais. 1(1). 2-20, 2009.

SCHNEIER, Bruce. **Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World**. 2016.

TOMAINO, B. et. al. **Metodologia científica: fundamentos, métodos e técnicas**. Rio de Janeiro: Freitas Bastos, 2016.