ATA DE APRESENTAÇÃO DE DEFESA DE TRABALHO DE CONCLUSÃO DO CURSO DE DIREITO

Aos dois dias do mês de outubro de dois mil e vinte e cinco, às treze horas, realizou-se virtualmente através da plataforma Google Meet, ID da reunião: https://meet.google.com/wfb-yxxa-rzw, a sessão pública da Banca Examinadora de Defesa de TCC, para conclusão do Curso de Direito, intitulado "Proteção de dados e responsabilidade civil das marketplaces no ambiente digital", apresentada pelo(a) acadêmico(a) Liz Camila Insfran Rios, para obtenção do título de Bacharel em Direito. A Banca Examinadora, composta pelos membros Bruno Marini, Presidente; Tarsis Witley, membro; Tiago Marino, membro, procedeu à arguição pública do(a) candidato(a), estando o(a) acadêmico(a):

(x) APROVADO(A) ( ) APROVADO(A) COM RESSALVAS ( ) REPROVADO(A)

Proclamado o resultado pelo presidente da Banca Examinadora, foram encerrados os trabalhos, dos quais, para constar, foi conferida e assinada a presente Ata pelos membros da Banca Examinadora e pelo(a) acadêmico(a).

Bruno Marini
(Presidente)

Tarsis Witley
(Membro)

Tiago Marino
(Membro)

Liz Camila Insfran Rios
(Acadêmico(a))

Documento assinado eletronicamente por **Tiago Marino**, **Professor do Magisterio Superior - Substituto**, em 20/10/2025, às 14:35, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Tarsis Witley de Almeida Arruda**, **Coordenador(a) Administrativo(a)**, em 20/10/2025, às 14:36, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Bruno Marini**, **Professor do Magisterio Superior**, em 20/10/2025, às 14:36, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **LIZ CAMILA INSFRAN RIOS**, **Usuário Externo**, em 20/10/2025, às 14:45, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufms.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5914559** e o código CRC **3457550E**.

FACULDADE DE DIREITO
Av Costa e Silva, s/nº - Cidade Universitária
Fone: (67) 3345-7145 / 3345-7251
CEP 79070-900 - Campo Grande - MS

PROTEÇÃO DE DADOS E RESPONSABILIDADE CIVIL DAS MARKETPLACES NO AMBIENTE DIGITAL

Liz Camila Insfran Rios

Orientador: Bruno Marini

RESUMO:

O presente trabalho busca analisar a responsabilidade civil das marketplaces frente à proteção de dados pessoais na era digital, examinado à luz da Lei Geral de Proteção de Dados (LGPD) e do Código de Defesa do Consumidor. No contexto de ampla inovação trazida pelo comércio eletrônico — que eliminou barreiras espaciais e temporais, facilitando o acesso do consumidor a inúmeros fornecedores —, surgem novas formas de vulnerabilidade, especialmente relacionadas à circulação e tratamento de dados pessoais. Dessa forma, este estudo tem como objetivo geral analisar a responsabilidade civil dos marketplaces frente à proteção dos dados pessoais de consumidores, destacando de que forma as plataformas digitais devem responder a incidentes como o vazamento de informações. Além disso, são discutidas as inovações, vantagens e desafios das marketplaces atuais, considerando sua posição como intermediadoras e a evolução legislativa voltada a fortalecer a proteção do consumidor e da privacidade informacional. A pesquisa utiliza metodologia bibliográfica, dedutiva e descritiva analisando artigos científicos, legislação, jurisprudência e doutrina especializada. Como resultado constatou-se que há desafios e avanços na proteção dos consumidores frente à coleta, ao armazenamento e ao compartilhamento massivo de dados pessoais, destacando a necessidade de adaptação das plataformas digitais às exigências legais e à responsabilidade civil, contribuindo para o fortalecimento de um ambiente de confiança e segurança nas relações digitais.

Palavras-chave: Proteção de dados no Marketplace. Lei Geral de Proteção de Dados. Responsabilidade Civil das plataformas.

ABSTRACT:

This study aims to analyze the civil liability of marketplaces regarding the protection of personal data in the digital era, examined in light of the Brazilian General Data Protection Law (LGPD) and the Consumer Defense Code. Within the context of significant innovations brought by electronic commerce—which has eliminated spatial and temporal barriers, making it easier for consumers to access numerous suppliers—new forms of vulnerability have emerged, particularly related to the circulation and processing of personal data. Thus, this work investigates the extent to which digital platforms should be held liable for damages caused to consumers, whether from improper exposure of data or failures in its protection. In addition, the study discusses the innovations, advantages, and challenges of current marketplaces, considering their position as intermediaries and the legislative evolution aimed at strengthening consumer protection and information privacy. The research employs a bibliographical methodology, analyzing scientific articles, legislation, case law, and specialized doctrine. Accordingly, it seeks to offer a critical reflection on the challenges and advances in consumer protection concerning the collection, storage, and widespread sharing of personal data, highlighting the need for

digital platforms to adapt to legal requirements and civil liability, thereby contributing to the strengthening of trust and security in digital relationships.

Keywords: Data Protection in Online Marketplaces. Brazilian General Data Protection Law (LGPD). Civil Liability of Digital Platforms.

INTRODUÇÃO

As transformações tecnológicas das últimas décadas impactaram profundamente a comunicação, a interação social e, especialmente, as relações de consumo, favorecendo a expansão do mercado para o ambiente virtual. O comércio eletrônico, especialmente por meio dos marketplaces, consolidou-se como alternativa dinâmica para fornecedores e consumidores, proporcionando facilidade na contratação e acesso ampliado a produtos, independentemente de fronteiras geográficas.

Nesse cenário, surgem também novas vulnerabilidades para o consumidor, marcadas pela ausência de contato físico com o produto e, principalmente, pela exposição de dados pessoais a processos amplos de coleta, armazenamento e tratamento por diversos agentes digitais. Tais mudanças, embora tragam praticidade e comodidade, impõem desafios significativos à proteção de dados e à segurança jurídica das transações, exigindo constante atualização das práticas jurídicas. O aumento das contratações online intensificou essas vulnerabilidades, tornando imprescindível a análise das normas protetivas e das obrigações dos intermediadores, como os marketplaces.

O crescente volume de contratações via internet intensifica essas questões e torna indispensável a análise do arcabouço normativo aplicável à proteção do usuário e à responsabilidade dos intermediadores dessas relações, como os marketplaces. Por isso, é fundamental examinar não apenas a legislação específica, como o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados (LGPD), mas também a eficácia das normas tradicionais diante das peculiaridades do comércio digital, avaliando como o ordenamento jurídico brasileiro busca se adaptar e harmonizar a proteção do consumidor com os avanços tecnológicos.

Este trabalho tem por objetivo analisar a responsabilidade civil dos marketplaces frente à proteção dos dados pessoais de consumidores, destacando de que forma as plataformas digitais devem responder a incidentes como o vazamento de informações. Ao longo da pesquisa, serão abordados conceitos e fundamentos da LGPD, as espécies de

responsabilidade civil, a identificação dos agentes de tratamento e a modalidade de responsabilidade aplicável a cada qual.

A responsabilidade civil, fundamento de proteção e equilíbrio nas relações jurídicas, está disciplinada nos artigos 927 a 954 do Código Civil de 2002[1], complementada pelo Código de Defesa do Consumidor e, mais recentemente, pela LGPD. O estudo aprofundado desses dispositivos, aliado à análise das especificidades das plataformas digitais, é imprescindível para delinear os limites e a natureza da responsabilidade dos agentes envolvidos no novo cenário varejista.

A relevância do tema se evidencia diante dos frequentes episódios de vazamento de dados no ambiente digital, ressaltando a importância de disciplinar a coleta e o tratamento das informações e, sobretudo, de definir e impor a responsabilização dos agentes que não asseguram a integridade do direito fundamental à proteção de dados pessoais.

Para tanto, este estudo está dividido em três tópicos: o primeiro detalha a conceituação e o funcionamento dos marketplaces; o segundo explora o dever de proteção de dados, a LGPD e o uso de inteligência artificial; e o terceiro analisa a responsabilidade civil dessas plataformas perante o consumidor e a legislação de dados.

1 CONCEITO E FUNCIONAMENTO DAS MARKETPLACES

No contexto da economia digital, o termo "marketplace" (do inglês, "local de vendas") designa uma plataforma virtual que centraliza a oferta de bens e serviços de múltiplos fornecedores para uma vasta base de usuários (Barbosa, 2021, p. 38). Diferenciando-se de um site de vendas tradicional, que comercializa produtos de uma única empresa, o marketplace atua como um intermediador, permitindo que diversos lojistas e até mesmo pessoas físicas exponham e comercializem seus produtos em um único ambiente digital. Essa natureza colaborativa visa o lucro mútuo, beneficiando-se da captação de clientes e do aumento de transações para toda a plataforma.

Do ponto de vista econômico, os marketplaces operam como mercados de múltiplos lados, gerando efeitos de rede: a atração de mais vendedores aumenta o valor

[1] Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
Art. 954. A indenização por ofensa à liberdade pessoal consistirá no pagamento das perdas e danos que sobrevierem ao ofendido, e se este não puder provar prejuízo, tem aplicação o disposto no parágrafo único do artigo antecedente.

para os compradores, e vice-versa, criando um ciclo virtuoso de crescimento. Os *marketplaces* assumem grande parte da complexidade operacional do comércio eletrônico, como o processamento de pagamentos, a gestão de fraudes, e, em muitos casos, até mesmo a logística e o atendimento ao cliente. Isso permite que o empreendedor digital concentre seus esforços no que faz de melhor: o desenvolvimento de produtos, a gestão de estoque e a inovação.

A arquitetura operacional de um marketplace é complexa e compreende etapas como o cadastro e verificação de vendedores (incluindo validações KYC e aceitação de termos), a publicação de ofertas e integração de catálogo, e a otimização da descoberta e recomendação de produtos. O processamento de pedidos e pagamentos (com *split* e antifraude), a orquestração logística (coleta, *fulfillment* e rastreio), e o pós-venda (com políticas de devolução, reembolso e mediação de disputas) são igualmente cruciais. Cada uma dessas etapas é meticulosamente desenhada para reduzir a assimetria de informação, inibir fraudes, padronizar expectativas e, fundamentalmente, elevar a confiança entre todas as partes envolvidas (Barbosa, 2021)

Para os varejistas, o marketplace oferece acesso a uma audiência ampliada e a uma marca com credibilidade, eliminando a necessidade de grandes investimentos em infraestrutura própria ou marketing em larga escala. Para os consumidores, a principal vantagem reside na conveniência e praticidade, como sintetizado por Daniel Sampaio:

> Para os usuários, o marketplace representa mais praticidade. Afinal, ele pode ver, em um único site, ofertas de vários vendedores. Assim, é possível comparar e escolher o melhor preço facilmente. Além disso, ele pode comprar de várias lojas diferentes e efetuar apenas um pagamento, em vez de passar por múltiplos processos de pagamento em vários sites. Enquanto isso, para os lojistas, ele é sinônimo de colaboração. Anunciando seus produtos nos marketplaces, as empresas– grandes ou pequenas– ganham mais visibilidade e conseguem alavancar as vendas (Sampaio, 2018).

A singularidade desse modelo reside no conceito de "*one-stop-shop*", que implica a concentração de todas as operações de compra – da busca ao fechamento do pedido – em um único sítio eletrônico (Grandes, 2013, p. 54). Isso significa que, no modelo de marketplace puro, não há redirecionamento dos consumidores para outras plataformas, mantendo a experiência de compra centralizada. Consequentemente, o consumidor se torna cliente direto do marketplace, mesmo que a entrega seja realizada pelo lojista fornecedor, o que reforça a responsabilidade da plataforma na gestão da experiência e na garantia da segurança da transação. Exemplos notáveis incluem Amazon, eBay, B2W e Mercado Livre.

A compreensão aprofundada desses mecanismos é essencial para analisar os desafios e as responsabilidades inerentes à proteção de dados no ambiente digital

1.1 Modelos de negócios em marketplaces: B2B, B2C, C2C e D2C

A compreensão dos diferentes modelos de negócios que operam dentro ou em conjunto com essas plataformas é fundamental para analisar as implicações em termos de proteção de dados e responsabilidade civil.

Conforme elucidado por Grandes (2013), um e-marketplace é um espaço virtual elaborado para viabilizar a oferta de bens e serviços, distinguindo-se de um e-commerce tradicional por ser uma plataforma administrada por uma empresa intermediadora, na qual diversos lojistas podem se registrar e comercializar. Essa agregação de ofertas pode se manifestar em diferentes formatos, cada um com suas particularidades de interação e público-alvo, quais sejam, Business-to-Business (B2B), Business-to-Consumer (B2C), Consumer-to-Consumer (C2C) e Direct-to-Consumer (D2C).

Inicialmente, o modelo business-to-business (B2B) refere-se às transações comerciais realizadas exclusivamente entre empresas. No contexto dos *marketplaces*, isso significa plataformas dedicadas à compra e venda de produtos, matérias-primas, componentes ou serviços entre organizações. Essas transações são frequentemente caracterizadas por volumes maiores, negociações mais complexas, contratos de longo prazo e a necessidade de integração de sistemas (Grandes, 2013)

O modelo B2C, ou *Business-to-Consumer*, é a forma mais comum e amplamente reconhecida de comércio eletrônico, envolvendo transações diretas entre empresas e consumidores finais. Nos *marketplaces* B2C, empresas de diversos portes e segmentos oferecem seus produtos e serviços diretamente ao público, aproveitando a infraestrutura e o alcance da plataforma. Este modelo é o cerne da discussão sobre proteção de dados e responsabilidade civil, pois lida diretamente com dados pessoais de milhões de indivíduos (Mascarenhas, 2018, p. 19).

O modelo C2C, ou *Consumer-to-Consumer*, facilita as transações entre consumidores individuais, onde a plataforma de *marketplace* atua como um intermediário que conecta compradores e vendedores (Mascarenhas, 2018, p. 44). Exemplos clássicos incluem plataformas de leilões ou de venda de itens usados, onde o foco está na interação

entre pares. No Brasil, o mercado livre se destaca como o marketplace com maior relevância, que possibilita a venda não só por empresas, mas também por pessoas físicas.

Pertinente pontuar que embora a plataforma não seja a vendedora direta, ela é responsável por prover um ambiente seguro para que as transações ocorram. A proteção de dados aqui se estende a ambos os lados da transação (comprador e vendedor), que são indivíduos, e a responsabilidade da plataforma pode ser invocada em casos de fraudes ou uso indevido de dados facilitados pela falha na segurança do ambiente.

Por fim, o modelo D2C, ou *Direct-to-Consumer*, representa uma estratégia na qual fabricantes ou marcas vendem seus produtos diretamente aos consumidores finais, sem a intermediação de varejistas tradicionais ou distribuidores. Embora não seja um tipo de *marketplace* em si, muitas marcas D2C utilizam *marketplaces* como um canal adicional de vendas, estabelecendo suas "lojas oficiais" dentro dessas grandes plataformas (Oliveira, 2025). Este modelo enfatiza a construção de um relacionamento direto com o cliente, permitindo uma coleta de dados mais aprofundada e personalizada, o que, por sua vez, exige um rigor ainda maior na conformidade com a LGPD.

Em suma, a diversidade de modelos de negócios em *marketplaces* reflete a complexidade do ambiente digital. Cada modelo apresenta desafios específicos em relação à proteção de dados e à delimitação da responsabilidade civil, exigindo uma análise aprofundada das interações e dos fluxos de informação para garantir a segurança e a privacidade dos usuários, em conformidade com a LGPD e o Código de Defesa do Consumidor.

1.2 O impacto dos marketplaces no empreendedorismo digital

Os *marketplaces* transcenderam a mera função de canais de venda, consolidando-se como catalisadores e transformadores do cenário do empreendedorismo digital. Ao oferecerem uma infraestrutura robusta e um vasto alcance de mercado, essas plataformas exercem um impacto multifacetado, especialmente para pequenas e médias empresas (EPPs) e novos empreendedores. A informação, como principal matéria-prima da economia digital, é o cerne desse novo ambiente, que se estabelece como uma ferramenta de expansão mercadológica.

Uma das contribuições mais significativas dos *marketplaces* é a democratização do acesso ao comércio eletrônico. Tradicionalmente, a entrada no varejo online exigia

investimentos consideráveis em desenvolvimento de plataforma, segurança, marketing e logística. Os *marketplaces* eliminam ou reduzem drasticamente muitas dessas barreiras, permitindo que empreendedores, mesmo com recursos limitados, iniciem suas operações digitais. Cada vez mais vemos o crescimento da chamada "cauda longa", que abriga milhares de pequenos lojistas especializados nos mais diversos nichos de mercado: artigos para bebê, produtos de pet shop, aluguel de filmes online, artigos de pesca e assinatura mensal de vinhos são apenas algumas das ofertas que podem ser encontradas pela internet no Brasil.

A facilidade de acesso e o baixo custo operacional são frequentemente destacados. O SEBRAE (2024) reforça que os *marketplaces* têm gerado oportunidades para pequenos negócios, justamente por conta desta variedade de produtos e serviços. Ao integrar-se a um *marketplace*, o empreendedor ganha acesso imediato a uma audiência muito maior do que conseguiria alcançar por conta própria. Plataformas com milhões de acessos mensais oferecem uma visibilidade e um potencial de vendas que seriam inatingíveis para um site individual. Essa característica é crucial para o surgimento de mais empresas virtuais, estimulando o comércio eletrônico e a regularização de negócios que, de outra forma, teriam dificuldades em se estabelecer.

Além disso, a expansão da internet e o crescimento do mercado de IA dependem da disponibilidade de dados, que são usados para criar perfis de comportamento e compra, direcionar publicidade e fornecer sugestões de produtos (Oliveira, 2022). Essa capacidade de análise de dados, oferecida pelos *marketplaces*, permite aos empreendedores refinar suas ofertas para nichos específicos, aumentando a eficácia de suas estratégias.

Por fim, essa relação simbiótica exige que os empreendedores compreendam tanto as oportunidades quanto os desafios, especialmente no que tange à conformidade com as normas de proteção de dados e à gestão da sua responsabilidade no ambiente digital.

2 DO DEVER DE PROTEÇÃO DE DADOS DAS MARKETPLACES

A ascensão dos *marketplaces* como pilares do empreendedorismo digital e do comércio eletrônico trouxe consigo uma complexidade inerente ao tratamento de dados pessoais. Essas plataformas, por sua natureza, atuam como ecossistemas onde milhões de interações diárias geram um volume massivo e diversificado de informações sobre consumidores, vendedores e suas transações. Nesse cenário, o dever de proteção de dados emerge como uma obrigação central e inegável para os *marketplaces*, não apenas como

uma exigência legal, mas como um pilar fundamental para a construção da confiança e a sustentabilidade dos negócios na era digital.

Este dever transcende a mera conformidade regulatória, enraizando-se no reconhecimento da proteção de dados pessoais como um direito fundamental, conforme abstraído na Constituição Federal brasileira (art. 5º, X e LXXIX). Ele impõe aos *marketplaces* a responsabilidade de garantir que toda e qualquer operação envolvendo dados pessoais, desde a coleta e o armazenamento até o processamento, compartilhamento e descarte, seja realizada de forma transparente, segura, ética e em estrita observância à legislação vigente.

Assim, a proteção de dados nos *marketplaces* envolve uma compreensão aprofundada da Lei Geral de Proteção de Dados (LGPD), a mitigação dos riscos associados à personalização algorítmica e a implementação rigorosa de práticas de *compliance* digital para prevenir vazamentos e assegurar a integridade das informações

2.1. A Lei Geral de Proteção de Dados (LGPD) e o tratamento de informações em marketplaces

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 de 2018, representa um marco regulatório fundamental no Brasil, estabelecendo diretrizes claras para o tratamento de dados pessoais, tanto em meios físicos quanto digitais. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) europeu, seu objetivo primordial é salvaguardar os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural (Pinheiro, 2020).

Para garantir essa proteção, a LGPD estabelece uma série de princípios fundamentais para o tratamento de dados. Ele deve ter propósitos legítimos, específicos e informados ao titular, sendo compatível com a finalidade e limitado ao mínimo necessário (Pinheiro, 2020). Isso implica que, por exemplo, marketplaces não podem coletar dados excessivos ou utilizá-los para fins não previamente comunicados.

Toda a cadeia de consumo deve ser transparente, informando claramente ao titular quem são os agentes envolvidos e como seus dados são compartilhados. Além disso, é imperativo que os marketplaces adotem medidas técnicas e administrativas robustas para proteger os dados de acessos não autorizados e incidentes (Pinheiro, 2020).

A compreensão dos elementos da relação de coleta e tratamento de dados passa, também, pela distinção dos papéis dos agentes de tratamento. A LGPD define especificamente o Controlador e o Operador, o que é crucial para delimitar as responsabilidades no contexto de um marketplace. O controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (Bruno, 2020). Em um marketplace, a própria plataforma geralmente atua como controladora em relação aos dados de seus usuários (compradores e vendedores) que coleta para fins de cadastro, navegação, marketing e gestão da própria plataforma, pois ela decide "o que" e "para que" esses dados serão tratados.

Por outro lado, o operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Um vendedor que utiliza o marketplace para comercializar seus produtos pode ser considerado um operador quando processa dados de clientes da plataforma para fins de entrega ou pós-venda, agindo conforme as instruções do marketplace. Contudo, o vendedor também pode ser um controlador independente em relação aos dados que coleta diretamente de seus próprios clientes fora do ambiente do marketplace ou para finalidades específicas de seu negócio.

A LGPD confere aos titulares dos dados uma série de direitos essenciais, como o direito de acesso, correção, eliminação, anonimização, bloqueio e portabilidade dos dados, bem como a revogação do consentimento (Pinheiro, 2020, p. 144). Para os marketplaces, isso implica a necessidade de desenvolver mecanismos eficazes para atender a essas solicitações dos usuários, garantindo a autonomia dos titulares sobre suas informações.

Nesse cenário de proteção e controle, o Artigo 7º da LGPD elenca dez condições específicas (bases legais) que tornam legítimo o tratamento de informações pessoais. É importante notar que basta que uma dessas condições seja cumprida para que o tratamento e a coleta de dados sejam considerados válidos. Embora o consentimento seja uma base legal importante, não é a única, e os marketplaces precisam gerenciar múltiplas bases para diferentes finalidades de tratamento (Bruno, 2020).

O consentimento do titular (inciso I) é frequentemente apontado como um elemento primordial e amplamente utilizado para justificar o tratamento de dados. No entanto, sua aplicação não é a única nem sempre suficiente, visto que o titular se encontra

em uma posição de vulnerabilidade particular. Nesse contexto, não é adequado atribuir a ele a responsabilidade exclusiva pela validação do processo de tratamento de dados, conforme argumenta Bioni (2020). Conforme estabelecido no Artigo 5º, inciso XII, da LGPD, o consentimento representa a manifestação clara, informada e voluntária do titular permitindo que seus dados pessoais sejam processados. Trata-se da decisão efetiva do indivíduo sobre quais tipos de dados serão utilizados em cada operação, e qualquer forma de coerção ou pressão para sua obtenção torna-o inválido (Brasil, 2018).

Em conjunto com o consentimento, a transparência é um requisito indispensável, evidenciando a boa-fé do controlador dos dados. A manifestação do consentimento deve ocorrer antes que a coleta dos dados pessoais seja iniciada, com o Artigo 9º da LGPD detalhando as informações que precisam ser fornecidas aos titulares de forma prévia, clara e visível sobre o ciclo completo do tratamento, a finalidade, a forma e o período de duração, a identificação do agente de tratamento, suas responsabilidades, os direitos do titular e os possíveis riscos. O titular pode, a qualquer momento, revogar seu consentimento, solicitando a exclusão de seus dados daquele tratamento.

2.2. O uso de inteligência artificial e algoritmos para personalização de ofertas e riscos jurídicos

A Inteligência Artificial (IA) e os algoritmos tornaram-se ferramentas indispensáveis para os *marketplaces*, impulsionando a personalização de ofertas e a otimização da experiência do usuário. A IA, definida como a capacidade de um programa de computador em executar funções e raciocínio comparáveis aos processos mentais humanos, permite que sistemas aprendam e melhorem sem programação explícita, identificando padrões em grandes volumes de dados (Peixoto, 2019).

Nos *marketplaces*, a IA e os algoritmos são amplamente empregados para recomendar produtos com base no histórico de navegação e compras, realizar precificação dinâmica em tempo real, direcionar publicidade de forma segmentada e otimizar os resultados de busca, visando aprimorar a experiência do consumidor e aumentar a eficiência econômica.

Contudo, o uso intensivo de IA e algoritmos para personalização acarreta riscos jurídicos e éticos significativos, particularmente no que concerne à proteção de dados e aos direitos dos consumidores. A personalização eficaz demanda a coleta e o

processamento de um volume substancial de dados pessoais, frequentemente sem o consentimento claro e informado do usuário.

Observa-se que a facilidade de transferência e acesso a dados, especialmente os altamente pessoais, pode resultar em violações do direito à privacidade, que é um bem jurídico fundamental protegido pela legislação. Exemplos como as "Robocalls", que utilizam dados pessoais obtidos sem consentimento, evidenciam a fragilidade dos dados em uma sociedade interconectada (A inteligência artificial e a Lei Geral de proteção de dados, 2023, p. 11).

Além disso, os algoritmos podem explorar vulnerabilidades psicológicas dos consumidores, levando a decisões de compra viciadas e minando a autonomia e a liberdade de escolha do indivíduo. Companhias já tratam dados sem o consentimento dos usuários para explorar a cognição e aumentar vendas, agravando a vulnerabilidade do consumidor ao captar estímulos psicológicos sem autorização (Schroder, 2023, p. 12).

Outro risco é a discriminação algorítmica, onde algoritmos treinados com dados históricos podem perpetuar vieses sociais, resultando em tratamento desigual para certos grupos de consumidores. A simples divulgação de informações sobre processos automatizados pode, paradoxalmente, "perpetuar assimetrias de poder existentes, ampliar vulnerabilidades de grupos marginalizados e subverter a privacidade dos indivíduos" (A inteligência artificial e a Lei Geral de proteção de dados, 2023, p. 2).

A falta de transparência e explicabilidade dos sistemas de IA, muitas vezes opacos e de difícil compreensão, dificulta a fiscalização e a responsabilização em caso de danos, desafiando o princípio da transparência da LGPD (A inteligência artificial e a Lei Geral de proteção de dados, 2023, p. 16). A LGPD estabelece a responsabilidade do controlador e do operador por danos patrimoniais, morais, individuais ou coletivos causados pelo tratamento de dados em violação à lei.

No contexto da IA, é um desafio jurídico complexo determinar a responsabilidade por danos algorítmicos, ressaltando a "necessidade de supervisão humana contínua para garantir a tomada de decisões éticas e a consideração de impactos sociais e ambientais" (A inteligência artificial e a Lei Geral de proteção de dados, 2023, p. 13).

2.3. Meios de prevenção a vazamentos de dados e práticas de *Compliance* Digital

Em um cenário onde a informação é o "ativo mais precioso na era do conhecimento" e a "principal causa para o vazamento de informações são as próprias ações humanas" (Pinheiro, 2020, p. 530), a prevenção a vazamentos de dados e a implementação de práticas robustas de *compliance* digital tornam-se imperativos para *marketplaces* e qualquer organização que trate dados pessoais.

A Lei Geral de Proteção de Dados (LGPD) reforça essa necessidade ao estabelecer que os agentes de tratamento devem adotar "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

O *compliance* digital, nesse contexto, vai além da mera conformidade legal, abrangendo um trabalho contínuo e abrangente de "blindagem digital" que visa disseminar o uso consciente e responsável das tecnologias (Pinheiro, 2020). As medidas técnicas constituem a base da segurança da informação, buscando proteger a confidencialidade, integridade e disponibilidade dos dados (Pinheiro, 2020).

Para *marketplaces*, isso inclui a criptografia, essencial para proteger dados em trânsito e em repouso, com a utilização de chaves criptográficas para garantir o sigilo das transações e a identificação (Pinheiro, 2020). A implementação de controles de acesso rigorosos, seguindo o "princípio do menor privilégio", garante acesso apenas ao estritamente necessário para cada função, estendendo-se a funcionários, terceirizados e parceiros (Pinheiro, 2020, p. 281).

E mais, o monitoramento contínuo e as auditorias são cruciais para identificar e reagir a ataques, sendo a auditoria legal de risco o primeiro passo para identificar vulnerabilidades (Pinheiro, 2020, p. 282). A realização periódica de testes de vulnerabilidade e simulações, como os testes de invasão (*black bag*)[2], permite identificar falhas de segurança antes que sejam exploradas (Pinheiro, 2020).

Além disso, sistemas de detecção de intrusão (IDS/IPS) e *firewalls* atuam como barreiras de segurança contra acessos não autorizados, e a existência de um plano de

[2] Black bag — operações militares de infiltração com objetivo de sabotagem ou furto e/ou extração de pessoas. Simulação de black bag é a alocação de um indivíduo, terceiro ou não, para testar tanto a segurança lógica como física e diagnosticar os pontos falhos.

backup e continuidade de negócios (PCN) é essencial para garantir a recuperação de dados e a continuidade das operações em caso de incidentes graves (Pinheiro, 2020)

Paralelamente às medidas técnicas, o *compliance* digital exige a criação de uma cultura de segurança e proteção de dados em toda a organização. Campanhas e treinamentos regulares para todos os funcionários, terceirizados e gestores são cruciais para disseminar a cultura de segurança e o uso responsável da tecnologia, visando formar um "usuário digitalmente correto" (Pinheiro, 2020). A gestão de riscos e a governança envolvem o planejamento estratégico, a revisão de contratos com fornecedores e parceiros, e a elaboração de minutas que tratem das responsabilidades quanto aos riscos digitais, abrangendo decisões que envolvem a aceitação, redução e transferência, orientando a escolha dos melhores controles e seus respectivos níveis de maturidade.

Um plano de resposta a incidentes é essencial para minimizar danos em caso de violação, incluindo ações, SLAs, registro e coleta de provas legais, e respostas rápidas. A criação de canais de denúncia anônimos fomenta a ética e a segurança e a classificação da informação é vital para determinar o nível de proteção necessário para cada tipo de dado. Por fim, a guarda adequada de provas eletrônicas, como *logs* de acesso e e-mails originais, é crucial para comprovar autoria e servir como prova em demandas judiciais, sendo a gestão eletrônica de documentos (GED) e a definição de tabelas de temporalidade fundamentais (Pinheiro, 2020).

A figura do Encarregado de Dados (DPO), estabelecida pela LGPD, é fundamental nesse processo, atuando como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). O DPO é essencial para garantir a conformidade da organização à LGPD, supervisionando a implementação das medidas de proteção e prestando esclarecimentos.

Em suma, a prevenção a vazamentos de dados e a efetividade do *compliance* digital em *marketplaces* dependem de uma abordagem multifacetada que combine tecnologia de ponta, políticas internas claras, educação contínua dos colaboradores e uma governança robusta.

3 RESPONSABILIDADE CIVIL DAS MARKETPLACES

A ascensão do comércio eletrônico transformou profundamente as relações de consumo, introduzindo novos modelos de negócio como os *marketplaces*. Estes se

consolidam como plataformas online que agregam ofertas de diversos vendedores, atuando como intermediários na negociação, pagamento e, por vezes, até na logística. No entanto, essa intermediação complexa, aliada à inerente vulnerabilidade do consumidor no ambiente digital, marcada pela desmaterialização e despersonalização da relação, levanta um desafio jurídico fundamental: a determinação da responsabilidade civil em caso de vícios, defeitos ou inadimplemento contratual.

Historicamente, o Direito do Consumidor já previa a responsabilização solidária dos fornecedores que integram a cadeia de consumo (Benjamin; Marques; Bessa, 2020, p. 150). No contexto dos *marketplaces*, a doutrina e a jurisprudência têm reconhecido a legitimidade dessas plataformas para responderem por contratempos nas transações mediadas, fundamentando essa responsabilidade na Teoria do Risco da Atividade e no dever de segurança do serviço prestado.

Assim, a discussão central reside em como aplicar os princípios protetivos do Código de Defesa do Consumidor (CDC) e do Código Civil a esses novos arranjos comerciais, distinguindo o papel do *marketplace* de um mero provedor de busca e garantindo a efetiva reparação dos danos ao consumidor.

3.1. Responsabilidade civil no contexto da relação de consumo

A responsabilidade civil, em sua essência, é a obrigação de reparar um dano causado a outrem, seja ele patrimonial ou moral (Gonçalves, 2017, p. 33). No âmbito das relações de consumo, este instituto adquire contornos específicos, moldados pela premissa fundamental da vulnerabilidade do consumidor. O Código de Defesa do Consumidor (CDC), Lei nº 8.078 de 1990, é o marco legal que estabelece um microssistema protetivo, reconhecendo a posição de fragilidade do consumidor diante do fornecedor.

Historicamente, a responsabilidade civil baseava-se na prova da culpa do agente (teoria subjetiva). Contudo, a complexidade das relações de consumo e a produção em massa impulsionaram a adoção da responsabilidade civil objetiva para os fornecedores. Conforme o CDC, o fornecedor responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços ou por vícios de produtos (Benjamin; Marques; Bessa, 2020, p. 128).

Essa mudança reflete a Teoria do Risco da Atividade, segundo a qual aquele que se beneficia da atividade econômica deve arcar com os riscos a ela inerentes. Um pilar central da responsabilidade civil consumerista é a solidariedade entre todos os participantes da cadeia de fornecimento. O CDC estabelece que "tendo mais de um autor a ofensa, todos responderão solidariamente pela reparação dos danos previstos nas normas de consumo" (Benjamin; Marques; Bessa, 2020, p. 127). Isso significa que o consumidor pode acionar qualquer um dos elos da cadeia fabricante, produtor, construtor, importador ou comerciante para buscar a reparação, facilitando o acesso à justiça e garantindo a efetividade da proteção.

A jurisprudência brasileira tem reiteradamente aplicado esses princípios ao ambiente digital, consolidando o entendimento sobre a responsabilidade de plataformas e intermediários. Em casos de falha na prestação de serviço ou não entrega de mercadoria, os tribunais têm afastado a ilegitimidade passiva de plataformas de reservas e de pagamentos, reconhecendo sua responsabilidade solidária e objetiva na cadeia de consumo.

Nesse sentido, o Tribunal de Justiça de Mato Grosso do Sul (TJ-MS) tem se posicionado de forma clara:

> Em decisão recente, o TJ-MS reconheceu a responsabilidade solidária de uma plataforma digital de reservas de hospedagem por falha na prestação de serviço, configurando dano moral. A Corte destacou a aplicação dos artigos 18, caput, e 25, § 1º, do CDC, que tratam da responsabilidade por vício do produto ou serviço e da solidariedade na cadeia de fornecimento (TJ-MS, Apelação Cível n. 08397635920238120001, Relatora: Juíza Sandra Regina da Silva Ribeiro Artioli, 4ª Câmara Cível, julgado em 30/04/2025, Data de Publicação: 05/05/2025).

Outro julgado do TJ-MS afastou a ilegitimidade passiva de uma plataforma de pagamento virtual, reconhecendo sua responsabilidade solidária pela não entrega de mercadoria e ausência de estorno do valor pago, o que caracterizou dano moral. A decisão fundamentou-se na interpretação do parágrafo único do artigo 7º do CDC, que integra a plataforma à cadeia de consumo por auferir rendimentos da intermediação (TJ-MS, Apelação Cível n. 08012559620238120016, Relator: Juiz Vitor Luis de Oliveira Guibo, 2ª Câmara Cível, julgado em 12/09/2024, Data de Publicação: 16/09/2024).

Reforçando esse entendimento, um agravo de instrumento do TJ-MS, envolvendo uma compra de produto pela internet com intermediação de empresa de pagamentos *on-*

line (Mercado Pago), afastou a ilegitimidade passiva da intermediadora e verificou sua responsabilidade solidária e objetiva, citando precedentes do Superior Tribunal de Justiça (STJ) que corroboram a falha na prestação do serviço e a não restituição do pagamento (TJ-MS, Agravo de Instrumento n. 14123006220248120000, Relator: Des. Amaury da Silva Kuklinski, 3ª Câmara Cível, julgado em 12/09/2024, Data de Publicação: 16/09/2024).

Essas decisões demonstram a tendência do judiciário em proteger o consumidor no ambiente digital, aplicando a teoria do risco e o princípio da solidariedade a todos os agentes que se beneficiam da cadeia de fornecimento, incluindo os intermediários. Além disso, o CDC prevê a inversão do ônus da prova em favor do consumidor, especialmente quando sua alegação for verossímil ou ele for hipossuficiente (Benjamin; Marques; Bessa, 2020, p. 120). Isso alivia a carga probatória do consumidor, que muitas vezes não possui o conhecimento técnico ou os meios para comprovar a culpa do fornecedor. Os danos passíveis de reparação incluem tanto os patrimoniais (materiais) quanto os morais, individuais, coletivos e difusos (Benjamin; Marques; Bessa, 2020, p. 126).

No contexto do comércio eletrônico, esses princípios são plenamente aplicáveis. A vulnerabilidade do consumidor no ambiente digital é, inclusive, acentuada pela desmaterialização da relação e pela assimetria informacional (Schroder, 2023). Portanto, a responsabilidade civil nas relações de consumo online busca assegurar que os direitos fundamentais do consumidor sejam protegidos, promovendo a confiança e a segurança necessárias para o desenvolvimento do mercado digital.

3.2. Lei do E-commerce (Decreto 7.962/2013) e exigências legais para marketplaces

O Decreto nº 7.962 de 2013, conhecido como a "Lei do E-commerce", foi editado para regulamentar o Código de Defesa do Consumidor (CDC) nas transações online, com o objetivo de fortalecer a confiança do consumidor e garantir sua proteção no ambiente virtual. Embora promulgado antes da plena ascensão dos *marketplaces*, suas disposições são diretamente aplicáveis a essas plataformas, que se enquadram na modalidade de contratação eletrônica.

As principais exigências legais impostas pelo Decreto, e que se estendem aos *marketplaces*, concentram-se em três pilares: o dever de informar, o atendimento facilitado ao consumidor e o respeito ao direito de arrependimento. Primeiramente, o dever de informar, previsto no Art. 2º do Decreto, exige que as plataformas

disponibilizem, em local de destaque e de fácil visualização, informações cruciais sobre o fornecedor e a oferta. Isso abrange desde o nome empresarial e número de inscrição (CNPJ/CPF) até o endereço físico e eletrônico, passando pelas características essenciais do produto ou serviço – incluindo seus riscos à saúde e segurança – e a discriminação de quaisquer despesas adicionais, como frete e seguros. Além disso, todas as condições integrais da oferta, como modalidades de pagamento, disponibilidade e prazos de entrega, devem ser claramente apresentadas.

Em segundo lugar, o atendimento facilitado ao consumidor, conforme o Art. 4º, impõe que o fornecedor ofereça um serviço adequado e eficaz em meio eletrônico. Esse serviço deve permitir que o consumidor envie e receba comunicações, incluindo notificações, reclamações e solicitações de cancelamento, com a garantia de confirmação imediata do recebimento da aceitação da oferta e a disponibilização do contrato em formato que permita sua conservação e reprodução.

Por fim, o direito de arrependimento, detalhado no Art. 5º, reforça o que já está previsto no art. 49 do CDC. As plataformas devem informar de forma clara e ostensiva os meios para o consumidor exercer seu direito de desistir da compra em até 7 (sete) dias, a contar da assinatura do contrato ou do recebimento do produto/serviço. É fundamental que o *marketplace* também comunique imediatamente a instituição financeira para que o estorno do valor seja processado sem ônus ao consumidor.

Apesar de ser um ato regulamentar e, portanto, não poder inovar na criação de direitos ou sanções não previstos em lei, o Decreto nº 7.962 de 2013 estabeleceu um patamar mínimo de transparência e proteção para o e-commerce. A inobservância de suas diretrizes pode acarretar a aplicação das sanções já previstas no CDC (Teixeira, 2015, p. 82), reforçando a importância de sua observância para a segurança jurídica e a confiança nas relações de consumo digitais.

3.3. Responsabilidade civil dos marketplaces em caso de violação da LGPD

A Lei Geral de Proteção de Dados (LGPD), Lei nº13.709/2018, trouxe um novo paradigma para o tratamento de dados pessoais no Brasil, impondo obrigações rigorosas aos agentes de tratamento de dados, incluindo os *marketplaces* (Pinheiro, 2021, p.25). Esses *marketplaces*, ao intermediar transações e coletar dados de usuários e vendedores, são considerados controladores ou operadores de dados pessoais, conforme definido pela LGPD (Art.5º, VI e IX).

Em caso de violação da LGPD, os *marketplaces* podem ser responsabilizados civilmente por danos causados aos titulares de dados, sejam eles materiais ou morais, individuais ou coletivos (LGPD, Art. 42). A responsabilidade civil é objetiva, ou seja, independe da existência de culpa, bastando a ocorrência do dano e a relação de causalidade entre o dano e a atividade de tratamento de dados (LGPD, Art. 42, §1º).

Nesses termos, quando ocorre uma falha na segurança da infraestrutura do *marketplace* que resulte na exposição indevida de dados de cadastro (nome, CPF, endereço, telefone) ou até mesmo dados de pagamento de milhares de usuários, a plataforma pode ser responsabilizada pelos danos decorrentes da violação, mesmo que não tenha havido dolo, em razão da responsabilidade objetiva e do dever de garantir a segurança da informação (LGPD, Art. 46).

A LGPD estabelece que o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar (Schreiber, 2020). Assim, a inobservância dessas diretrizes, seja por falhas de segurança, coleta indevida, uso ou compartilhamento sem base legal adequada, ou desrespeito aos direitos dos titulares, pode acarretar severas sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD) e, principalmente, a obrigação de indenizar os titulares pelos danos sofridos.

CONSIDERAÇÕES FINAIS

O avanço tecnológico e a consolidação do comércio eletrônico, especialmente por meio dos *marketplaces*, transformaram profundamente as relações de consumo, oferecendo conveniência e acesso sem precedentes. Contudo, essa digitalização também acentuou a vulnerabilidade do consumidor, que se vê diante de assimetrias informacionais e complexidades operacionais inerentes ao ambiente virtual. Nesse cenário, a proteção do consumidor, inicialmente balizada pelo Código de Defesa do Consumidor (CDC), exigiu adaptações e complementos normativos para garantir a segurança e a equidade nas transações online.

O Decreto nº 7.962 de 2013, conhecido como a "Lei do E-commerce", representou um esforço inicial para regulamentar as relações de consumo no ambiente digital sob a égide do CDC. Ao estabelecer diretrizes claras sobre o dever de informar, o atendimento facilitado e o direito de arrependimento, o Decreto buscou mitigar os riscos e fortalecer a confiança do consumidor. Embora essencial, sua natureza regulamentar impôs limites à

sua abrangência, não sendo suficiente para cobrir todas as nuances e desafios emergentes da era digital, especialmente aqueles relacionados ao tratamento de dados pessoais.

Nesse contexto, a Lei Geral de Proteção de Dados (LGPD) surgiu como um marco fundamental, preenchendo lacunas e impondo um novo patamar de responsabilidade aos *marketplaces*. Ao qualificá-los como controladores ou operadores de dados, a LGPD estabeleceu a responsabilidade objetiva por danos decorrentes de violações, como vazamentos, coleta excessiva ou uso e compartilhamento indevidos de informações. Essa legislação reforça a importância da segurança, da transparência e do consentimento, garantindo aos titulares o controle sobre seus dados e impondo sanções administrativas severas em caso de descumprimento.

Em suma, a proteção do consumidor no ambiente dos *marketplaces* é um desafio multifacetado que exige a atuação conjunta e harmonizada de diferentes diplomas legais. A intersecção entre o CDC, o Decreto do E-commerce e a LGPD é crucial para assegurar que a inovação tecnológica ocorra em consonância com os direitos fundamentais dos indivíduos. A contínua adaptação do arcabouço jurídico e a vigilância das autoridades são indispensáveis para promover um ambiente digital seguro, confiável e justo para todos os participantes.

REFERÊNCIAS

BARBOSA, Gabriel Luciano Almeida. O comércio eletrônico e a responsabilidade civil dos marketplaces. 2021. Monografia (Graduação em Direito) — Centro Universitário São Judas Tadeu (CSJT), Santos, 2021.

BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. Manual de direito do consumidor. 8. ed. São Paulo: Revista dos Tribunais, 2017.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 11 set. 2025.

BRASIL. Decreto nº 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm Acesso em: 11 set. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm Acesso em: 11 set. 2025.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. Lei geral de proteção de dados comentada. 2. ed. rev. atual e ampl. São Paulo: Thomson Reuters Brasil, 2020.

DINIZ, Maria Helena. Curso de direito civil brasileiro: responsabilidade civil. 35. ed. São Paulo: Saraiva, 2021. v. 7.

GRANDES, Luisa Ancona. Relacionamentos no varejo eletrônico: um estudo de caso sobre o marketplace e seus parceiros. 2013. Dissertação (Mestrado Profissional em Gestão Internacional) — Escola de Administração de Empresas de São Paulo, Fundação Getulio Vargas, São Paulo, 2013.

GONÇALVES, Carlos Roberto. Direito civil: responsabilidade civil. 12. ed. São Paulo: Saraiva Educação, 2017.

OLIVEIRA, Bruno de. Tipos de e-commerce: conheça os 13 principais e como funcionam. 2025. Disponível em: https://ecommercenapratica.com/blog/tipos-de-e-commerce/. Acesso em: 15 set. 2025.

OLIVEIRA, I. B. A inteligência artificial e o impacto da LGPD. 2022. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade Evangélica de Goiás, Anápolis, 2022. Disponível em: http://repositorio.aee.edu.br/handle/aee/20029. Acesso em: 11 set. 2025.

PEIXOTO, F. H.; SILVA, R. Z. M. Inteligência artificial e direito. Curitiba: Alteridade, 2019.

PINHEIRO, Patricia Peck. Proteção de dados pessoais: comentários à lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

SEBRAE. Conheça as vantagens do e-marketplace para os pequenos negócios. 2017. Disponível em: http://www.sebrae.com.br/sites/PortalSebrae/artigos/conheca-as-vantagens-do-e-marketplace-para-os-pequenos negocios,3f6402b5b0d36410VgnVCM1000003b74010aRCRDx. Acesso em: 15 set. 2025.

SCHREIBER, Anderson. Direito e inteligência artificial: aspectos jurídicos da inteligência artificial. Rio de Janeiro: Forense, 2020.

TEIXEIRA, Tarcisio. Direito digital e processo eletrônico. 5. ed. São Paulo: Saraiva Educação, 2020.

TJ-MS. Apelação Cível n. 08397635920238120001. Relatora: Juíza Sandra Regina da Silva Ribeiro Artioli. 4ª Câmara Cível, Campo Grande, MS, julgado em 30 abr. 2025, publicado em 5 maio 2025.

TJ-MS. Apelação Cível n. 08012559620238120016. Relator: Juiz Vitor Luis de Oliveira Guibo. 2ª Câmara Cível, Mundo Novo, MS, julgado em 12 set. 2024, publicado em 16 set. 2024.