



UNIALFA
CENTRO UNIVERSITÁRIO ALVES FARIA
MESTRADO PROFISSIONAL EM DIREITO CONSTITUCIONAL ECONÔMICO

CLÁUDIA OLIVEIRA BUENO

**A PROTEÇÃO DO CONSUMIDOR *ON-LINE*:
VULNERABILIDADE ALGORÍTMICA E DIGITAL**

GOIÂNIA
2024

CLÁUDIA OLIVEIRA BUENO

**A PROTEÇÃO DO CONSUMIDOR *ON-LINE*:
VULNERABILIDADE ALGORÍTMICA E DIGITAL**

Dissertação de Mestrado apresentada ao curso de Mestrado Profissional do Centro Universitário Alves Faria (UNIALFA), como requisito parcial para a obtenção do grau de Mestre em Direito Constitucional Econômico.

Orientador: Prof. Dr. Diógenes Faria de Carvalho.

**GOIÂNIA
2024**

Catálogo na fonte: Biblioteca UNIALFA

B928p

Bueno, Cláudia Oliveira.

A proteção do consumidor on-line: vulnerabilidade algorítmica e digital.

/ Cláudia Oliveira Bueno. – 2024.

136 f.: 30cm.

Orientador: Prof. Dr. Diógenes Faria Carvalho.

Dissertação (Mestrado) – Programa de Pós-Graduação em Direito Constitucional Econômico, Centro Universitário Alves Faria (UNIALFA) – Goiânia, 2024.

1. Comércio eletrônico. 2. Regulação Econômica. 3. Dark Patterns. 4. Constituição Econômica. I. Carvalho, Diógenes Faria. II. UNIALFA. III. Título.

CDU: 366.4+004.738.5:339

UNIALFA
CENTRO UNIVERSITÁRIO ALVES FARIA
MESTRADO PROFISSIONAL EM DIREITO CONSTITUCIONAL ECONÔMICO

Folha de aprovação da dissertação apresentada ao curso de Mestrado Profissional em Administração do Centro Universitário Alves Faria como requisito para a obtenção do título de Mestre.

Aprovada em de 2024

Banca Examinadora

Prof. – Orientador

Prof.– Avaliador UNIALFA

Prof.– Avaliador Externo

AGRADECIMENTOS

Chegar até este momento foi uma jornada que envolveu não apenas dedicação acadêmica, mas também o apoio inestimável de inúmeras pessoas que, direta ou indiretamente, contribuíram para que este trabalho se tornasse realidade.

Agradeço primeiramente ao meu orientador, Dr. Diógenes Faria de Carvalho, cuja paciência, dedicação e expertise foram fundamentais ao longo de todo o processo. Suas orientações não apenas enriqueceram esta pesquisa, mas também moldaram a maneira como encaro desafios acadêmicos e profissionais. Estendo minha gratidão aos membros da banca, Dra. Maria Luiza Baillo Targa e Dr. André Perin Schmidt Neto, pelas valiosas contribuições e observações que aprimoraram este trabalho.

Sou profundamente grata aos colegas e professores do curso de Mestrado Profissional do Centro Universitário Alves Faria – UNIALFA, que enriqueceram minha experiência acadêmica por meio de discussões instigantes e críticas construtivas. Cada troca de ideias, cada debate e cada momento compartilhado foram essenciais para o amadurecimento desta pesquisa e para o meu desenvolvimento pessoal e profissional.

À minha família, expresso minha eterna gratidão. Vocês foram minha maior motivação para persistir e alcançar meus objetivos. Um agradecimento especial ao meu cônjuge, Rogério, que esteve ao meu lado em todos os momentos, celebrando as conquistas e me apoiando nos desafios. Sua paciência, compreensão e incentivo foram pilares fundamentais para que eu seguisse em frente. Obrigada por ser meu porto seguro, por acreditar nos meus sonhos e por compartilhar comigo cada etapa desta jornada.

A todos que, de alguma forma, contribuíram para a concretização deste trabalho, meu sincero agradecimento.

LISTA DE QUADROS

Quadro 1– Conceito de diversos autores sobre vulnerabilidade digital.....	45
--	-----------

LISTA DE SIGLAS E ABREVIATURAS

ANPD - Autoridade Nacional de Proteção de Dados

CCPA - Lei de Privacidade do Consumidor da Califórnia (California Consumer Privacy Act)

CDC - Código de Defesa do Consumidor

CMA - Competition and Markets Authority

CNIL - Comissão Nacional de Informática e Liberdades (Commission Nationale de l'Informatique et des Libertés)

DMA - Ato dos Mercados Digitais (Digital Markets Act)

DSA - Ato de Serviços Digitais (Digital Services Act)

EC - Comissão Europeia (European Commission)

EDPB - Conselho Europeu de Proteção de Dados (European Data Protection Board)

EUA - Estados Unidos da América

FTC - Comissão Federal de Comércio (Federal Trade Commission)

GDPR - Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation)

IA - Inteligência Artificial

LGPD - Lei Geral de Proteção de Dados

OMC - Organização Mundial do Comércio

RGPD - Regulamento Geral sobre a Proteção de Dados

SBDC - Sistema Brasileiro de Defesa da Concorrência

RESUMO

Esta dissertação examina as vulnerabilidades enfrentadas pelos consumidores no comércio eletrônico, com foco nas práticas abusivas, como os *dark patterns* e o uso inadequado de dados pessoais. A pesquisa explora como o avanço da digitalização influencia o comportamento do consumidor por meio de algoritmos invisíveis, que comprometem a autonomia e a privacidade dos usuários, tornando-os suscetíveis à manipulação. Inserida na linha de pesquisa Desenvolvimento Econômico e Princípios Constitucionais da Ordem Econômica, a dissertação enfatiza a necessidade de regulamentação específica no comércio eletrônico, capaz de acompanhar a rápida evolução tecnológica e proteger os consumidores contra práticas enganosas e invasivas. No Brasil, observam-se lacunas significativas na legislação, exigindo adaptações para garantir segurança e transparência nas relações digitais. A comparação com legislações internacionais, como o GDPR europeu, evidencia a necessidade de diretrizes rigorosas para assegurar o consentimento informado e a proteção da privacidade. A metodologia adotada consistiu em uma pesquisa bibliográfica qualitativa, orientada pelo método dedutivo. A revisão bibliográfica permitiu construir um panorama teórico sobre as vulnerabilidades digitais e práticas abusivas no comércio eletrônico. A abordagem qualitativa possibilitou uma análise interpretativa das questões jurídicas e sociais, explorando como os *dark patterns* e a manipulação algorítmica afetam o direito à privacidade e à liberdade de escolha. O método dedutivo foi aplicado para discutir a adequação das normas existentes à proteção do consumidor digital, com base em princípios gerais como os direitos de privacidade e autonomia. Os resultados indicam que a manipulação algorítmica e o uso de *dark patterns* são práticas que limitam a liberdade de escolha dos consumidores, expondo uma lacuna regulatória no Brasil. A pesquisa sugere que o país pode beneficiar-se ao adotar diretrizes preventivas, inspiradas em regulamentações internacionais, para proteger os consumidores contra abusos no ambiente digital. Conclui-se que uma regulamentação mais abrangente e transparente é essencial para garantir um mercado digital ético e equilibrado, que valorize a dignidade e os direitos fundamentais dos consumidores.

Palavras-chave: Comércio eletrônico. Regulação Econômica. Dark Patterns. Consolidação Econômica. Vulnerabilidade digital do consumidor.

ABSTRACT

This dissertation examines the vulnerabilities faced by consumers in e-commerce, focusing on abusive practices such as dark patterns and the improper use of personal data. The research explores how the advancement of digitalization influences consumer behavior through invisible algorithms that compromise users' autonomy and privacy, making them susceptible to manipulation. Embedded in the research line of Economic Development and Constitutional Principles of Economic Order, the dissertation emphasizes the need for specific regulation in e-commerce capable of keeping pace with rapid technological evolution and protecting consumers from deceptive and invasive practices. In Brazil, significant legislative gaps are observed, requiring adaptations to ensure security and transparency in digital relations. A comparison with international regulations, such as the European GDPR, highlights the need for strict guidelines to ensure informed consent and privacy protection. The methodology adopted consisted of qualitative bibliographic research guided by the deductive method. The bibliographic review provided a theoretical overview of digital vulnerabilities and abusive practices in e-commerce. The qualitative approach enabled an interpretative analysis of legal and social issues, exploring how dark patterns and algorithmic manipulation affect the right to privacy and freedom of choice. The deductive method was applied to discuss the adequacy of existing regulations to protect digital consumers, based on general principles such as privacy and autonomy rights. The results indicate that algorithmic manipulation and the use of dark patterns are practices that limit consumers' freedom of choice, exposing a regulatory gap in Brazil. The research suggests that the country could benefit from adopting preventive guidelines inspired by international regulations to protect consumers from abuses in the digital environment. It concludes that more comprehensive and transparent regulation is essential to ensure an ethical and balanced digital market that values consumers' dignity and fundamental rights.

Keywords: E-commerce. Economic Regulation. Dark Patterns. Economic Constitution. Digital Consumer Vulnerability.

SUMÁRIO

INTRODUÇÃO	12
1 COMÉRCIO ELETRÔNICO E A PROTEÇÃO DO CONSUMIDOR	17
1.1 A SOCIEDADE DA INFORMAÇÃO OU SOCIEDADE EM REDE	17
1.2 NOVAS DINÂMICAS DAS PRÁTICAS COMERCIAIS A PARTIR DA SOCIEDADE EM REDE	24
1.2.1 Novos produtos.....	35
1.2.2 Novos serviços	39
1.3 A VULNERABILIDADE DO CONSUMIDOR NO COMÉRCIO ELETRÔNICO ..	42
1.3.1 Vulnerabilidade digital	42
1.3.2 Vulnerabilidade algorítmica.....	48
1.3.3 Vulnerabilidade na proteção de dados	52
2 DARK PATTERNS: ABUSO DA PRIVACIDADE E ASSÉDIO AO CONSUMIDOR NO COMÉRCIO ELETRÔNICO.....	56
2.1 <i>DARK PATTERNS</i>	56
2.1.1 Conceito e origem	56
2.1.2 Aspectos gerais: assimetria de <i>design</i>	61
2.2 LEGISLAÇÃO DO DIREITO ESTRANGEIRO SOBRE A UTILIZAÇÃO DE <i>DARK PATTERNS</i>	67
2.3 PRIVACIDADE E AUTONOMIA DO CONSUMIDOR: CONCEITOS NECESSÁRIOS E FRAGILIZAÇÃO DIANTE DOS <i>DARK PATTERNS</i> NO COMÉRCIO ELETRÔNICO	73
2.4 PRINCÍPIOS ORIENTADORES E DIRETRIZES ÉTICAS DO GUIA Nº 3/2022 DA EDPB	78
3 IMPACTOS DO DESENVOLVIMENTO DE FERRAMENTAS DE DESIGN PARA MANIPULAÇÃO DA INFORMAÇÃO NO COMÉRCIO ELETRÔNICO.....	82
3.1 IMPACTOS DO DESENVOLVIMENTO DE FERRAMENTAS DE DESIGN PARA MANIPULAÇÃO DA INFORMAÇÃO NA AUTODETERMINAÇÃO INFORMATIVA.....	82
3.2 <i>DARK PATTERNS</i> : DIGITAL MARKET ACT, DIGITAL SERVICES ACT (DSA) E SEUS IMPACTOS NA PROTEÇÃO DE DADOS	89
3.3 MARCOS LEGAIS NACIONAIS E INTERNACIONAIS DE PROTEÇÃO AO CONSUMIDOR NO AMBIENTE DIGITAL.....	97
3.4 ANÁLISE COMPARATIVA DOS DIREITOS DO CONSUMIDOR: LEGISLAÇÃO	

BRASILEIRA VERSUS DIGITAL MARKET ACT 105

CONSIDERAÇÕES FINAIS 119

REFERÊNCIAS 123

INTRODUÇÃO

A crescente digitalização das relações de consumo transformou profundamente o comércio e a forma como produtos e serviços são ofertados e adquiridos. No ambiente do comércio eletrônico, as barreiras físicas se dissolvem, permitindo que consumidores acessem uma ampla variedade de opções com apenas alguns cliques. Essa facilidade e conveniência, contudo, vêm acompanhadas de novos desafios e riscos, especialmente em relação à privacidade e segurança dos dados pessoais. Com o avanço acelerado da tecnologia, torna-se essencial entender como o ordenamento jurídico pode proteger os consumidores diante de práticas algorítmicas que, muitas vezes, se mostram exploratórias e manipulativas, impactando diretamente a autonomia e a confiança dos usuários.

No cenário contemporâneo, o uso de algoritmos e *big data* no comércio eletrônico levanta questões complexas relacionadas à vulnerabilidade digital. Segundo Marques e Mucelin, a vulnerabilidade digital pode ser entendida como uma extensão das vulnerabilidades tradicionais, porém agravada pelas características peculiares do ambiente digital, como a desmaterialização e desterritorialização das relações de consumo.¹ Empresas utilizam tecnologias sofisticadas para coletar, analisar e prever comportamentos dos consumidores, moldando as experiências de compra de maneiras que o próprio usuário desconhece. Essa manipulação invisível desafia o conceito tradicional de autonomia do consumidor, pois as decisões são influenciadas por processos algorítmicos que operam nos bastidores das plataformas digitais. Esse cenário levanta preocupações quanto ao direito de escolha e à transparência nos processos de coleta e uso de dados.

A vulnerabilidade do consumidor digital tornou-se um tema de extrema relevância, especialmente em uma era em que a vida cotidiana está cada vez mais conectada ao mundo digital. À medida que as práticas comerciais se adaptam aos avanços tecnológicos, consumidores se veem expostos a estruturas de poder assimétricas e dinâmicas de controle que favorecem as empresas. Assim, este estudo parte da hipótese de que o ordenamento jurídico brasileiro necessita de uma regulamentação específica para proteger o consumidor contra práticas algorítmicas

¹ MARQUES, Claudia Lima; MUCELIN, Guilherme. *A vulnerabilidade digital do consumidor no ciberespaço: novas perspectivas para a proteção de dados pessoais e o papel do direito do consumidor*. Revista de Direito do Consumidor, São Paulo, v. 134, p. 15-38, jan./fev. 2022.

abusivas que exploram sua vulnerabilidade digital e informacional. Essa hipótese orienta a escolha pelo método dedutivo, fundamentado na aplicação de princípios gerais do direito do consumidor e da privacidade para analisar os desafios específicos do comércio eletrônico.

Esta dissertação de Mestrado, apresentada ao curso de Mestrado Profissional do Centro Universitário Alves Faria (UNIALFA), insere-se na linha de pesquisa Desenvolvimento Econômico e Princípios Constitucionais da Ordem Econômica. Nesse contexto, o estudo aborda a questão central: como o direito brasileiro e comparado protege os consumidores contra práticas digitais abusivas que exploram a vulnerabilidade informacional e algorítmica? Essa indagação é especialmente relevante no Brasil, onde o Código de Defesa do Consumidor (CDC) ainda carece de disposições específicas que abordem a manipulação algorítmica e a proteção do consumidor digital.

O uso de algoritmos para influenciar as escolhas dos consumidores no comércio eletrônico não é uma prática isolada; trata-se de um fenômeno global. Em nível mundial, diversas empresas de e-commerce têm desenvolvido técnicas conhecidas como *dark patterns*² para direcionar o comportamento do usuário. Essas técnicas envolvem o *design* de interfaces digitais que enganam e manipulam consumidores, levando-os a realizar ações que, em um contexto mais transparente, poderiam não escolher. Ao analisar essa realidade, percebe-se a necessidade de compreender as implicações sociais e jurídicas dessas práticas, que não só afetam a experiência do consumidor, mas também podem comprometer a confiança pública no ambiente digital.

A relevância social do tema é evidente, à medida que a sociedade se torna mais dependente das tecnologias digitais, a proteção dos consumidores assume um papel crucial. A vulnerabilidade digital afeta consumidores de diferentes perfis, mas é especialmente prejudicial para aqueles que possuem menor conhecimento técnico. Grupos como jovens, idosos e consumidores de baixa renda estão entre os mais suscetíveis às armadilhas dos *dark patterns*, que exploram a falta de familiaridade com os mecanismos tecnológicos de manipulação. Dessa forma, é essencial que o debate jurídico contemple medidas que visem a proteção desses grupos vulneráveis, garantindo que todos possam usufruir das vantagens do comércio eletrônico sem

² BRIGNULL, Harry. *Dark Patterns*. 2010. Disponível em: <https://darkpatterns.org>. Acesso em: 12 ago. 2024.

correr o risco de serem manipulados.

Do ponto de vista jurídico, este estudo questiona a adequação das normativas existentes no Brasil e na União Europeia para lidar com a vulnerabilidade digital dos consumidores. O direito do consumidor, historicamente construído para proteger indivíduos em contextos físicos, enfrenta um desafio significativo ao tentar se adaptar ao ambiente digital. A introdução de regulamentos que considerem a proteção contra abusos algorítmicos torna-se, portanto, indispensável para garantir que as plataformas digitais operem de maneira transparente e responsável. Essa abordagem é necessária para equilibrar o desenvolvimento econômico e a proteção dos direitos dos consumidores, promovendo um ambiente digital seguro e confiável.

Este trabalho explora a complexidade da vulnerabilidade algorítmica e digital, propondo um debate sobre os limites da atuação empresarial na coleta e manipulação de dados dos consumidores. Ao observar o desenvolvimento de legislações internacionais, como o *Digital Markets Act* e o *Digital Services Act* da União Europeia, percebe-se a urgência de um arcabouço jurídico brasileiro que proteja efetivamente os consumidores contra essas práticas. Essa comparação também oferece insights sobre como o Brasil pode aprimorar suas leis para enfrentar os desafios e oportunidades apresentados pela digitalização do comércio.

A introdução dos *dark patterns* nas plataformas de comércio eletrônico revela um cenário de opacidade e manipulação, onde as escolhas dos consumidores são condicionadas por *designs* que exploram vieses cognitivos. Práticas como a renovação automática de assinaturas, a criação de urgências fictícias e a dificuldade em cancelar serviços são exemplos de como o *design* digital pode minar a liberdade de escolha. Tais práticas abusivas reforçam a necessidade de uma regulamentação que considere a ética e a transparência no *design* de interfaces, a fim de preservar a autonomia do consumidor e garantir a equidade nas relações de consumo digital.

O primeiro capítulo deste estudo analisa o desenvolvimento do comércio eletrônico e a transformação das práticas comerciais na era digital. Compreender como o comércio eletrônico evoluiu e como ele se insere na sociedade da informação é essencial para contextualizar o impacto das práticas algorítmicas na vulnerabilidade do consumidor. A digitalização dos processos comerciais trouxe benefícios significativos, como a conveniência e o acesso ampliado a produtos e serviços, mas também criou um ambiente propício para a exploração dos consumidores por meio da coleta e manipulação massiva de dados pessoais.

O segundo capítulo examina os *dark patterns* como formas de assédio ao consumidor no comércio eletrônico. Essas práticas de *design*, que podem parecer inofensivas à primeira vista, representam uma manipulação deliberada do comportamento do usuário. No contexto digital, onde as decisões dos consumidores são frequentemente baseadas em interações rápidas e impulsivas, os *dark patterns* exploram essa vulnerabilidade de maneira quase invisível, mascarando suas verdadeiras intenções sob uma aparência de conveniência e simplicidade. A compreensão dessas práticas e as legislações sobre sua utilização é fundamental para desenvolver estratégias que protejam os consumidores de influências maliciosas.

O terceiro capítulo discute o impacto das ferramentas de *design* manipulativas na proteção de dados pessoais e nos marcos legais nacionais e internacionais. O uso intensivo de algoritmos nas plataformas de *e-commerce* não apenas afeta as escolhas dos consumidores, mas também levanta questões sobre privacidade e segurança. A comparação entre a legislação brasileira e marcos regulatórios internacionais oferece uma visão abrangente dos desafios enfrentados pela proteção do consumidor e das oportunidades para fortalecer a regulamentação no Brasil.

A metodologia adotada neste trabalho é composta por uma pesquisa bibliográfica, de caráter qualitativo, orientada pelo método dedutivo. A pesquisa bibliográfica foi essencial para o levantamento e análise de material teórico relevante sobre as vulnerabilidades dos consumidores no comércio eletrônico e as práticas abusivas que comprometem a sua autonomia e privacidade. Conforme aponta Barral, a pesquisa bibliográfica permite construir um panorama amplo do conhecimento existente, utilizando livros, artigos científicos e legislações nacionais e internacionais. Através dessa abordagem, foi possível fundamentar teoricamente a necessidade de maior proteção ao consumidor frente ao avanço das tecnologias digitais e às práticas de manipulação algorítmica.³

A pesquisa qualitativa, por sua vez, possibilitou uma análise interpretativa e aprofundada das questões sociais e jurídicas envolvidas no tema. De acordo com Bittar, a abordagem qualitativa é adequada para compreender fenômenos que afetam a experiência humana e os valores sociais, como os que dizem respeito à privacidade e à liberdade de escolha no ambiente digital. Esse método é apropriado para explorar

³ BARRAL, Welber. Metodologia da pesquisa jurídica. Editora del Rey, 2007. p. 40.

as nuances dos *dark patterns* e o impacto da coleta de dados sobre o consumidor, buscando interpretar como esses elementos influenciam as relações de consumo e desafiam o direito à informação e à autonomia do usuário no comércio eletrônico.⁴

O método dedutivo orientou a análise jurídica ao partir de conceitos e princípios gerais, como os direitos fundamentais de privacidade e proteção ao consumidor, aplicando-os ao contexto específico do comércio eletrônico. Segundo Bittar, o método dedutivo é eficaz para estudos que visam aplicar teorias amplas em cenários concretos, contribuindo para o desenvolvimento de conclusões sobre a necessidade de regulamentações mais rigorosas. Dessa forma, a dissertação utiliza o método dedutivo para argumentar que, com base nos princípios de proteção do consumidor, o Brasil precisa adotar medidas mais abrangentes e preventivas, similares a legislações internacionais, para assegurar a segurança e a transparência nas relações de consumo digital.⁵

As contribuições deste trabalho se estendem além da análise teórica, propondo diretrizes para uma regulamentação mais ampla e eficaz no combate a práticas abusivas no comércio eletrônico. O papel do consumidor no ambiente digital é central para o desenvolvimento da economia contemporânea. No entanto, para que esse desenvolvimento ocorra de forma justa e equilibrada, é essencial que os direitos dos consumidores sejam respeitados. A manipulação algorítmica, ao comprometer a liberdade de escolha, contraria princípios fundamentais do direito do consumidor, sendo necessária uma abordagem jurídica que preserve a autonomia dos indivíduos no ambiente digital.

Este estudo busca, portanto, não apenas compreender a vulnerabilidade algorítmica, mas também demonstrar soluções jurídicas para enfrentá-la. A discussão sobre os direitos do consumidor no comércio eletrônico torna-se, assim, uma questão de cidadania digital, onde a proteção da privacidade e da liberdade de escolha deve ser assegurada por meio de regulamentações claras e eficazes. Ao promover o debate sobre a vulnerabilidade digital, espera-se que o trabalho contribua para o desenvolvimento de um comércio eletrônico mais ético e responsável, que valorize a dignidade e os direitos fundamentais do consumidor.

⁴ BITTAR, Eduardo CB. Metodologia da pesquisa jurídica. Saraiva Educação SA, 2016. p. 86.

⁵ BITTAR, Eduardo CB. Metodologia da pesquisa jurídica. Saraiva Educação SA, 2016. p. 88.

1 COMÉRCIO ELETRÔNICO E A PROTEÇÃO DO CONSUMIDOR

Este capítulo explora as transformações e desafios impostos pelo avanço da tecnologia e pela globalização digital nas práticas comerciais contemporâneas. No contexto da sociedade da informação, ou sociedade em rede, o comércio eletrônico se apresenta como uma realidade consolidada que demanda novas abordagens e regulamentações voltadas à proteção dos consumidores. A análise abrange o impacto das redes digitais nas dinâmicas de mercado, examinando a introdução de novos produtos e serviços que surgem nessa sociedade hiperconectada. Além disso, aborda as diversas formas de vulnerabilidade às quais os consumidores estão sujeitos nesse ambiente, incluindo a vulnerabilidade digital, algorítmica e na proteção de dados, destacando a necessidade de uma abordagem jurídica que proteja os direitos fundamentais do consumidor na era digital.

1.1 A SOCIEDADE DA INFORMAÇÃO OU SOCIEDADE EM REDE

A sociedade contemporânea vivencia uma transformação significativa impulsionada pelos avanços tecnológicos, que têm reduzido as barreiras espaciais e facilitado a comunicação entre pessoas em diferentes partes do mundo. O crescimento das comunicações e a troca de informações, especialmente com o uso da *internet*, têm promovido a globalização e moldado uma sociedade pós-moderna. Este período, conhecido como pós-modernidade, foi amplamente discutido por Lyotard em 1979, destacando a perda de força das grandes narrativas e a criação de novas formas de entender a realidade. A expansão da cibercultura e a intensificação do consumo de bens materiais e simbólicos caracterizam esta era, conforme discutido por Featherstone.⁶

A sociedade contemporânea demonstra uma redução das barreiras espaciais, pois pessoas em diferentes pontos do planeta podem se comunicar facilmente. Dessa forma, os avanços tecnológicos têm promovido o crescimento das comunicações e a troca de informações, especialmente com o uso da *internet*. Tudo isso impulsiona a globalização, refletindo em uma sociedade pós-moderna.

⁶ FEATHERSTONE, Mike. *Undoing culture: globalization, postmodernism and identity*. London: Sage, 1995. p. 115.

A sociedade da informação, conforme explorada por diversos autores, constitui um conceito central para a compreensão das transformações contemporâneas em escala global. Castells é um dos principais teóricos a abordar essa mudança, argumentando que a sociedade da informação é marcada pela ascensão das tecnologias da informação, que reconfiguram as interações sociais e econômicas em uma estrutura global de redes digitais. Esse fenômeno, segundo o autor, transcende a simples abundância de informação, sendo essencialmente uma transformação na maneira como o conhecimento e a informação são produzidos e utilizados, moldando novas formas de organização social e econômica.⁷

Bell também contribui significativamente para essa discussão, ao propor que a sociedade pós-industrial é caracterizada pela centralidade do conhecimento, que substitui os bens materiais como principal fonte de poder e inovação.⁸ No entanto, essa visão tem sido criticada por autores como Lyotard, que alerta para a mercantilização do conhecimento na sociedade da informação, onde o saber é frequentemente reduzido a meros dados processáveis pelas tecnologias digitais. Lyotard sugere que essa redução do conhecimento a um valor puramente utilitário reflete uma perda de seu conteúdo humanista e formativo, transformando-o em um produto destinado ao mercado.⁹

A transição para essa sociedade em rede, como descrita por Castells, envolve não apenas a informatização das atividades econômicas, mas também uma mudança estrutural na organização social. Ele argumenta que a economia informacional, que surge nas últimas décadas do século XX, opera através de redes globais de empresas e comunicação, onde a geração e o processamento da informação se tornam as principais fontes de produtividade e poder. Essa nova configuração econômica e social é marcada pela interconexão e pela fluidez das relações, onde as fronteiras nacionais se tornam menos relevantes diante da integração global das redes de informação.¹⁰

Drucker enfatiza que a sociedade da informação representa uma ruptura significativa com o modelo econômico anterior, centrado na produção industrial. Para

⁷ CASTELLS, M. *A sociedade em rede*. São Paulo: Paz e Terra, 1999. p. 77.

⁸ BELL, D. *O advento da sociedade pós-industrial: uma tentativa de previsão social*. São Paulo: Cultrix, 1978.

⁹ LYOTARD, Jean François. *A condição pós-moderna*. 5. ed. Rio de Janeiro: José Olympio, 2009. p. 5.

¹⁰ LYOTARD, Jean François. *A condição pós-moderna*. 5. ed. Rio de Janeiro: José Olympio, 2009. p. 79.

o autor, o conhecimento se torna a base da economia, sendo essencial para o desenvolvimento de novas tecnologias e para a competitividade das empresas no mercado global. Essa visão é compartilhada por outros teóricos, que veem na sociedade da informação uma nova era, onde a inovação e o progresso são impulsionados pelo domínio do conhecimento e pela capacidade de gerenciar e aplicar informações de maneira eficiente.¹¹

No entanto, essa transição para uma sociedade dominada pela informação e pelo conhecimento também levanta questões éticas e sociais. Lyotard critica a instrumentalização do saber na sociedade da informação, argumentando que essa tendência leva à alienação do conhecimento de seu contexto social e humano. Ele destaca que, na busca por eficiência e produtividade, a sociedade corre o risco de desumanizar o processo de aprendizado e de reduzir o conhecimento a uma simples mercadoria, disponível apenas para aqueles que podem pagar por ele.¹²

Por fim, Castells sugere que a sociedade da informação é um fenômeno em constante evolução, onde as redes digitais continuam a expandir sua influência em todas as esferas da vida social. Ele argumenta que, para entender plenamente o impacto dessas mudanças, é necessário reconhecer a centralidade da tecnologia na definição das novas formas de organização social e econômica. A sociedade da informação, portanto, não é apenas uma etapa no desenvolvimento humano, mas uma transformação profunda que redefine as bases da interação social e do poder em escala global.¹³

Nesse contexto, o cenário pós-moderno é predominantemente cibernético e informacional. Aumentam-se os estudos e pesquisas sobre a linguagem para entender melhor a mecânica de sua produção e compatibilidade com máquinas informáticas. Além disso, crescem as investigações sobre inteligência artificial (IA) e esforços sistemáticos para desvendar a estrutura e o funcionamento do cérebro, bem como o mecanismo da vida. Nesse ambiente, os esforços científicos, tecnológicos e políticos visam informatizar a sociedade. Embora o avanço e a popularização da

¹¹ DRUCKER, P. F. *Sociedade pós-capitalista*. São Paulo: Pioneira, 1994.

¹² LYOTARD, Jean François. *A condição pós-moderna*. 5. ed. Rio de Janeiro: José Olympio, 2009. p. 103.

¹³ CASTELLS, M. *A sociedade em rede*. São Paulo: Paz e Terra, 1999.

tecnologia informática tragam sérios reflexos, seu impacto sobre a ciência tem se mostrado significativo.¹⁴

À medida que o contato via redes sociais aumenta, as relações presenciais tendem a diminuir com o tempo. A cibercultura surge, portanto, como parte integrante da sociedade contemporânea, composta pela fusão do social e do tecnológico, resultando da interação diária dos seres humanos nos meios virtuais.¹⁵ Na proporção que o espaço cibernético se expande, percebe-se que a comunicação e a informação estão transformando o que era uma esfera informatizada em um local onde todos podem informar e serem informados. Isso ocorre porque, quando as mensagens se tornam interativas e as pessoas podem ser emissoras e receptoras, elas podem modificar ou ampliar as informações imediatamente.¹⁶

A interação humana no ciberespaço se tornou essencial, pois tudo ocorre por meio da informação. A cibercultura permite uma conexão social sem a necessidade de presença física, apoiada pelos mais recentes avanços tecnológicos. O ciberespaço, além de ser um ponto de encontro para interações humanas, exerce grande influência nas áreas econômicas e científicas, com potencial para se expandir para diversos outros campos. A universalização da cibercultura promove a co-presença e a interação de quaisquer pontos do espaço físico, social ou informacional.¹⁷

Assim, desde o início do século, observa-se uma transição de uma cultura predominantemente material para um novo paradigma tecnológico virtual, que só tem ganhado espaço graças à constante adaptação da sociedade e seu uso contínuo. Segundo Lévy, é virtual toda entidade desterritorializada, capaz de gerar várias manifestações concretas em diferentes momentos e lugares, sem estar vinculada a um local ou tempo específico.¹⁸

Além disso, destaca-se que a desmaterialização, ou seja, a possibilidade de realizar negócios eletronicamente sem a necessidade de presença física, é um dos

¹⁴ LYOTARD, Jean François. *A condição pós-moderna*. 5. ed. Rio de Janeiro: José Olympio, 2009. p. 104.

¹⁵ LEMOS, André. *Cibercultura: tecnologia e vida social na cultura contemporânea*. Porto Alegre: Sulina, 2008. p. 10.

¹⁶ LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 1999. p. 23.

¹⁷ LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 1999. p. 112.

¹⁸ LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 1999. p. 50.

principais fatores para o aumento da demanda no meio digital. Este fenômeno ocorre através de acordos de vontades mútuas, que transcendem as barreiras geográficas.¹⁹

Assim, a *internet* permite aos consumidores acessar uma ampla gama de produtos e serviços, além de facilitar a concretização de contratos. As noções tradicionais de contrato mudam no meio virtual, transformando-se em algo descentralizado, desterritorializado, desmaterializado e atemporal, constituindo uma evolução em relação às práticas de consumo tradicionais.²⁰

Dada a evolução tecnológica e a dominância das mídias digitais na vida cotidiana, além de seu contínuo crescimento, é impossível imaginar a vida moderna sem uma ampla variedade de informações e acesso à *internet*. De acordo com Sarmiento, a informação tornou-se a ferramenta mais essencial para o exercício e controle do poder, acesso a recursos materiais e imateriais valorizados pela sociedade, e o desenvolvimento da maioria das atividades humanas.²¹

Ferraz e Viola, em um artigo publicado pela Fundação Konrad Adenauer, sustentam que essa evidente dependência social do controle informativo deu origem ao que hoje se conhece como sociedade da informação.²² Martin descreve essa sociedade como uma na qual a qualidade de vida, assim como as perspectivas de transformação social e desenvolvimento econômico, dependem cada vez mais da informação e de sua exploração.²³

O avanço tecnológico, particularmente na *internet*, criou um ambiente favorável ao desenvolvimento dessa sociedade da informação, possibilitando a rápida coleta, cruzamento e disseminação de dados. Isso resulta em uma rede interconectada de divulgação imediata e irrestrita, gerando impactos positivos e negativos na vida cotidiana das pessoas, especialmente dos usuários.

As significativas revoluções sociais dos últimos séculos têm em comum o fato de cada uma, em seu período, ditar o funcionamento da economia. No momento atual de profunda mudança histórica, onde a informação e a *internet* ganham protagonismo,

¹⁹ MARQUES, Eduardo. *A desmaterialização do mundo: tecnologia e sociedade*. São Paulo: Annablume, 2004. p. 169.

²⁰ ROCHA, Rubens A.; ATZ, Neli. *Contratos eletrônicos: o comércio eletrônico e a segurança jurídica*. São Paulo: Saraiva, 2011. p. 4.

²¹ SARMENTO, Daniel. *Liberdades Comunicativas e Direito ao Esquecimento na ordem constitucional brasileira*. Parecer divulgado no ano de 2015. Disponível em: <http://www.migalhas.com.br/arquivos/2015/2/art20150213-09.pdf>. Acesso em: 30 de jun. 2024.

²² FERRAZ, José Eduardo Junqueira. VIOLA, Mario. *A Internet e Sociedade: Direito ao esquecimento*. Disponível em: <https://itsrio.org/wp-content/uploads/2017/06/Direito-ao-esquecimento.pdf>. Acesso em: 30 de jun. 2024.

²³ MARTIN, William J. *The Global Information Society*. Vermont: Brookfield, 1995.

surge uma nova economia, que se origina no final do século XX, e é descrita por Castells como informacional, global e em rede.²⁴

Essa economia é definida como informacional porque a produtividade e a competitividade dos agentes econômicos (sejam empresas, regiões ou países) dependem crucialmente da capacidade de gerar, processar e aplicar eficientemente o conhecimento. É global porque as principais atividades produtivas, de consumo e de circulação, bem como seus componentes (capital, trabalho, matérias-primas, administração, informação, tecnologia e mercados), estão organizadas em uma escala mundial, seja diretamente ou através de uma rede de conexões entre agentes econômicos. Além disso, é em rede porque, nas novas condições históricas, a produtividade é gerada e a competição ocorre em uma rede global de interações entre redes empresariais.²⁵

Dentro dessa nova estrutura social, a informação se torna o elemento central, uma fonte de valor social, político e econômico. Conforme Bioni, a informação assume “um papel central e definidor da sociedade”, funcionando como o novo elemento estruturante que reorganiza a sociedade, tal como a terra, as máquinas a vapor e a eletricidade fizeram nas sociedades agrícola, industrial e pós-industrial.²⁶

Neste novo paradigma, os dados pessoais também passam a ser mercantilizados. Além da monetização, essa nova configuração social altera a própria esfera relacional do indivíduo, com os dados sendo vistos não apenas como informações, mas como extensões da própria pessoa. É fundamental, portanto, não confundir “dado” com “informação”, apesar de alguns autores tratarem esses termos como sinônimos.

De acordo com Bioni, “o dado é o estágio bruto da informação”, pois não agrega conhecimento por si só. Dados são apenas fatos não processados que, quando organizados, tornam-se inteligíveis e permitem a extração de informação. Dados desorganizados representam um conjunto sem valor informativo. Assim, Bioni esclarece que a dinâmica de um banco de dados envolve a entrada (*input*), o

²⁴ CASTELLS, Manuel. *A sociedade em rede: do conhecimento à política*. In: CASTELLS, Manuel (Org.); CARDOSO, Gustavo (Org.). *Sociedade em Rede: Do conhecimento à ação política*. Lisboa: Imprensa Nacional, 2005. p. 68.

²⁵ CASTELLS, Manuel. *A sociedade em rede: do conhecimento à política*. In: CASTELLS, Manuel (Org.); CARDOSO, Gustavo (Org.). *Sociedade em Rede: Do conhecimento à ação política*. Lisboa: Imprensa Nacional, 2005. p. 69.

²⁶ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020. p. 5.

processamento e a saída (*output*) de informações. É essencial, portanto, o gerenciamento manual ou automatizado de um banco de dados para que se extraia algum conhecimento.²⁷

O termo "dado" está associado a algo menos elaborado do que a informação propriamente dita. Para Doneda, o dado está relacionado a uma espécie de pré-informação, anterior à interpretação e ao processamento. A informação, por outro lado, refere-se a algo além da mera representação contida no dado, atingindo o limiar da cognição.²⁸

Castells reinterpreta a tese da sociedade da informação em relação ao papel da informática, adaptando-a aos tempos modernos. Ele introduz o conceito de sociedade em rede, combinando informatização e globalização. A criação da realidade virtual, as mudanças na mídia, a transformação na percepção de espaço e tempo, e todas as questões econômicas e culturais são vistas como consequências do avanço e da disseminação das tecnologias da informação. O autor enfatiza a formação de uma teia social digital e interativa possibilitada por essas tecnologias. Segundo ele, a tendência histórica aponta para a organização dos principais processos sociais em redes (mercados financeiros, empresas, meios de comunicação, etc.), viabilizadas pela infraestrutura do paradigma informacional. Dessa forma, ele estende a discussão sobre as teses da sociedade da informação sem superá-las.²⁹

Em suma, é evidente a influência das tecnologias da informação na vida econômica e social. A questão está na proporção dada ao papel da tecnologia na definição das direções e formas sociais. Desde Bell, existe uma tendência de misturar informação, conhecimento e tecnologia. Bell advoga por um caráter pragmático e utilitário do conhecimento, transformando-o em tecnologia econômica e social. O próximo passo na evolução das teses sobre a nova sociedade é a tendência de considerar a tecnologia informática como a essência da sociedade.³⁰

Em seguida, a transformação do conhecimento/informação em sua capacidade

²⁷ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020. p. 31.

²⁸ DONEDA, Danilo Cesar Maganhoto. *Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

²⁹ CASTELLS, Manuel. *A sociedade em rede: do conhecimento à política*. In: CASTELLS, Manuel (Org.); CARDOSO, Gustavo (Org.). *Sociedade em Rede: Do conhecimento à ação política*. Lisboa: Imprensa Nacional, 2005. p. 87.

³⁰ NORA, Simon; MINC, Alain. *A informatização da sociedade*. Rio de Janeiro: Fundação Getúlio Vargas, 1980.

de digitalização é claramente expressa na vida digital por Negroponte³¹ e, finalmente, por Castells³², que destaca o informacionalismo, sublinhando a linguagem informática e sua capacidade de penetrar nas esferas sociais como fatores essenciais para a caracterização da mudança social.

O desenvolvimento das teses da sociedade da informação tende a valorizar a informática. Nesta nova sociedade, a importância não reside apenas no estreitamento da relação entre ciência e tecnologia, mas também na amplificação do papel mediador do mundo produtivo. A trajetória da concepção de conhecimento e informação nas teses da sociedade da informação mostra uma redução gradual do conteúdo significativo dessas noções. Inicialmente, o conhecimento é reduzido ao aspecto utilitário, e posteriormente, há uma redução ainda maior, quando o conhecimento é identificado com a linguagem da máquina informática. Assim, o saber relevante para a sociedade da informação passa a ser apenas aquele que pode ser codificado e aproveitado produtivamente.

A era pós-moderna, marcada pela constante evolução tecnológica e pela crescente importância da informação, reflete mudanças profundas na maneira como as pessoas interagem, consomem e realizam negócios. A transição para uma economia informacional, global e em rede, conforme descrito por Castells, destaca a centralidade da informação e a necessidade de processar e aplicar eficientemente o conhecimento para garantir a competitividade. Nesse contexto, a sociedade da informação redefine as práticas comerciais, introduzindo novas dinâmicas e exigências. Com a crescente desmaterialização das transações e a mercantilização dos dados pessoais, a maneira como se fazem negócios se transforma radicalmente, abrindo caminho para o próximo tópico: a evolução das práticas comerciais.

1.2 NOVAS DINÂMICAS DAS PRÁTICAS COMERCIAIS A PARTIR DA SOCIEDADE EM REDE

³¹ NEGROPONTE, Nicholas. *A vida digital*. São Paulo: Companhia das Letras, 1995. NETO, José Luíz Castro et al. Comércio eletrônico: análise dos fatores críticos. *Business Review*, v. 9, p. 1-25, 2010. p. 4.

³² CASTELLS, Manuel. *A sociedade em rede: do conhecimento à política*. In: CASTELLS, Manuel (Org.); CARDOSO, Gustavo (Org.). *Sociedade em Rede: Do conhecimento à ação política*. Lisboa: Imprensa Nacional, 2005. p. 36.

A evolução das práticas comerciais ao longo da história demonstra a crescente complexidade e sofisticação das relações de troca, especialmente no contexto da sociedade de consumo. Na era digital, a proteção ao consumidor enfrenta desafios inéditos devido ao uso intensivo de algoritmos, que não apenas personalizam as experiências, mas também aumentam a vulnerabilidade do consumidor. Esse processo cria uma “sociedade de crédito aberto” onde consumidores são incentivados a realizar compras e assumir dívidas que, muitas vezes, estão além de sua capacidade de pagamento, resultando em superendividamento e perpetuação de uma relação desigual no mercado digital.³³

Desde os primórdios, com o escambo nas economias de subsistência, até a ascensão do comércio eletrônico no século XXI, as formas de comércio têm se adaptado às necessidades e tecnologias de cada era. No contexto moderno, o comércio eletrônico revolucionou a maneira como consumidores e fornecedores interagem, ampliando o alcance dos mercados e facilitando transações sem barreiras geográficas. No entanto, essa transformação digital trouxe novos desafios, principalmente no que diz respeito à proteção do consumidor, que agora enfrenta vulnerabilidades algorítmicas e digitais que precisam ser adequadamente reguladas e monitoradas.

As práticas comerciais estão no cerne do Direito do Consumidor. Sua visibilidade, complexidade e mutabilidade, características da sociedade de consumo, representam um desafio significativo para o legislador. Segundo Sidou, um dos primeiros juristas a defender os direitos do consumidor no Brasil, o crescimento extraordinário do comércio e a ampliação da publicidade aumentaram significativamente a necessidade de proteção ao consumidor, a ponto de se tornar uma questão de segurança do Estado devido aos potenciais conflitos sociais que poderiam surgir, e que cabem ao Estado resolver.³⁴ Esse desenvolvimento do comércio resultou em um fenômeno desconhecido pelos economistas do passado: a sociedade de consumo, caracterizada pelo consumo pelo simples prazer de consumir e pela expansão da riqueza por sugestão consciente ou inconsciente.

A digitalização das práticas comerciais permitiu a criação de perfis de consumo que orientam o mercado de forma detalhada e estratégica, fazendo com que as

³³ SCHMIDT NETO, André Perin; AMARAL, Augusto Jobim do. *Governar pela dívida: o crédito na era dos algoritmos*. Revista de Direito do Consumidor, São Paulo, vol. 143, ano 31, set./out. 2022. p. 8.

³⁴ SIDOU, J. M. Othon. *Direito do Consumidor*. 2. ed. Rio de Janeiro: Forense, 1977.

empresas moldem suas ofertas e condições com base em dados coletados em larga escala. Essas informações podem direcionar a experiência do consumidor de modo a reforçar padrões de consumo contínuo e, em alguns casos, explorar vulnerabilidades financeiras, ampliando a necessidade de regulamentações que protejam os direitos dos consumidores no ambiente digital.³⁵

Definir práticas comerciais não é tarefa fácil. Dada a constante mudança do mercado, especialmente na era da sociedade de consumo, o que hoje se configura como prática comercial pode desaparecer ou se tornar irrelevante amanhã devido às transformações nas necessidades do mercado. É mais fácil, portanto, definir o que não são práticas comerciais, usando um critério de exclusão. Sob essa perspectiva negativa, as práticas comerciais se opõem às práticas de produção.

Simplificadamente, práticas comerciais são o resíduo da produção, ou seja, a fase pós-produção da sociedade de consumo. Os bens de consumo têm duas fases distintas: produção e comercialização, sendo as práticas comerciais relacionadas a esta última.³⁶

Historicamente, no início da civilização, as sociedades viviam sob uma economia de subsistência, onde a produção era voltada para o consumo próprio. Essas comunidades primitivas não conheciam o comércio e as relações de troca decorrentes dele. Com o desenvolvimento, a economia de subsistência tornou-se insuficiente para o sustento dos indivíduos. Assim, o primeiro e mais simples instrumento de intercâmbio foi a troca, onde os excedentes de um grupo eram trocados pelos de outro, conforme a necessidade mútua. Isso gerou problemas de equivalência entre os bens trocados, levando à criação de instrumentos de pagamento.

Com a Revolução Industrial, e a ascensão de uma nova classe social, o comércio floresceu sob bases liberais, impulsionado pela produção em escala e a consequente redução dos preços unitários. Isso demandou uma regulamentação sistemática, culminando no movimento de codificação. Esse boom econômico, entretanto, trouxe sérias consequências devido à falta de regulamentação, resultando em exploração dos trabalhadores, consumidores e do meio ambiente. Essas

³⁵ SCHMIDT NETO, André Perin; AMARAL, Augusto Jobim do. *Governar pela dívida: o crédito na era dos algoritarismos*. Revista de Direito do Consumidor, São Paulo, vol. 143, ano 31, set./out. 2022. p. 8.

³⁶ BENJAMIN, Antônio Herman de Vasconcellos e. *Curso de direito do consumidor*. São Paulo: Revista dos Tribunais, 2007.

questões, inicialmente negligenciadas, tornaram-se centrais para a manutenção da civilização, levando à intervenção do Direito na atividade econômica.³⁷

A partir do século XVII, surgiram os primeiros bancos comerciais privados, que começaram a emitir notas e recibos bancários, utilizados como papel-moeda. Alguns desses bancos monopolizavam a emissão de notas bancárias, atividade que levou ao surgimento de muitos bancos centrais, como o Banco da Inglaterra, fundado em 1694 por banqueiros privados para financiar os *déficits* da Coroa. Posteriormente, o Estado assumiu o monopólio da emissão do papel-moeda lastreado em ouro. Contudo, o ouro, por suas reservas limitadas, impunha um limite à oferta monetária, vinculando a emissão de moeda à quantidade de ouro disponível, o que se tornou um grande obstáculo à expansão do comércio internacional e das economias nacionais, sendo superado no século XX.³⁸

No início do século XIX, a mecanização da agricultura deslocou muitos trabalhadores agrícolas para o setor industrial emergente. Abandonando suas cabanas primitivas, esses trabalhadores migraram para os grandes centros industriais, impulsionados por novas tecnologias, o que levou à urbanização e ao surgimento de uma sociedade industrial.³⁹ A urbanização e a expansão das cidades, juntamente com o crescimento do comércio, criaram as condições materiais e intelectuais para a evolução do capitalismo. Em seu livro "A origem do capitalismo", a historiadora Wood discute o desenvolvimento do capitalismo, desafiando a ideia de sua naturalidade e apresentando-o como um elemento guiador da história.⁴⁰

Wood, alinhada às filosofias de Karl Marx e Karl Polanyi, define o capitalismo como um sistema onde bens e serviços, inclusive necessidades básicas, são produzidos para troca lucrativa; onde a capacidade humana de trabalho é uma mercadoria à venda; e onde a competição e a maximização do lucro são as regras fundamentais da vida.⁴¹ Essas regras caracterizam o capitalismo como um sistema focado no crescimento das forças produtivas e na elevação da produtividade do trabalho através de recursos técnicos avançados, com o objetivo de manter a

³⁷ COMPARATO, F. K. *A proteção ao consumidor na Constituição Brasileira de 1988*. Revista de Direito Mercantil, n. 80, 1990.

³⁸ MARCOS, R. M. F. *Companhias Pombalinas: contributo para a história das sociedades por acções em Portugal*. Coimbra: Almedina, 1997.

³⁹ TOFFLER, Alvin. *A terceira onda*. Rio de Janeiro: Editora Record, 1980.

⁴⁰ WOOD, Ellen Meiksins. *A origem do capitalismo*. Rio de Janeiro: Editora Jorge Zahar Editor, 2001. p. 79.

⁴¹ WOOD, Ellen Meiksins. *A origem do capitalismo*. Rio de Janeiro: Editora Jorge Zahar Editor, 2001. p. 80.

produção e a autoexpansão do capital.

As práticas de perfilização e uso de *big data* no comércio eletrônico transformam os consumidores em alvos constantes de ofertas personalizadas, promovendo um ciclo de consumo estimulado por algoritmos. Nesse contexto, é fundamental que o ordenamento jurídico acompanhe essas mudanças, garantindo a proteção dos direitos dos consumidores e promovendo um ambiente comercial equilibrado e ético, alinhado aos princípios constitucionais de proteção ao consumidor.⁴²

Concordando com Wood⁴³ e grandes teóricos como Karl Marx e Max Weber, o sociólogo Catani argumenta que o capitalismo não é apenas um sistema de produção de bens de consumo, mas um conjunto de práticas onde a força de trabalho é tratada como mercadoria. Para sustentar o capitalismo, é necessário que a propriedade dos meios de produção esteja concentrada nas mãos de uma classe social, enquanto outra classe depende da comercialização de sua força de trabalho para subsistir.⁴⁴

Em "O que é capitalismo", Catani afirma que a fase essencial da ascensão do capitalismo é representada pela 'Revolução Industrial'. Durante esse período, inovações técnicas colocaram a potência mecânica – inicialmente a energia hidráulica e, posteriormente, o vapor – a serviço da produção.⁴⁵ Isso transformou profundamente o processo produtivo, que deixou de ocorrer em casas ou oficinas artesanais para ser realizado em fábricas. Esse novo modelo de produção tornou-se coletivo, envolvendo dezenas ou até centenas de trabalhadores, em contraste com a produção individual ou de pequenos grupos que utilizavam ferramentas manuais.

No contexto da nova economia de rede, observa-se uma transformação radical nas práticas comerciais e sociais, onde o acesso a bens e serviços assume maior relevância do que a própria posse. Conforme apontado por Rifkin, o crescimento das redes digitais, a desmaterialização dos bens e a ascensão dos ativos intangíveis, como dados e conhecimento, são características definidoras dessa nova era.⁴⁶ As práticas comerciais passaram a se basear cada vez mais na troca de experiências e

⁴² SCHMIDT NETO, André Perin; AMARAL, Augusto Jobim do. *Governar pela dívida: o crédito na era dos algoritmos*. Revista de Direito do Consumidor, São Paulo, vol. 143, ano 31, set./out. 2022. p. 2.

⁴³ WOOD, Ellen Meiksins. *A origem do capitalismo*. Rio de Janeiro: Editora Jorge Zahar Editor, 2001. p. 80.

⁴⁴ CATANI, Afrânio Mendes. *O que é capitalismo*. São Paulo: Editora Brasiliense, 2011. p. 102.

⁴⁵ CATANI, Afrânio Mendes. *O que é capitalismo*. São Paulo: Editora Brasiliense, 2011. p. 102.

⁴⁶ RIFKIN, Jeremy. *A era do acesso: a transição de mercados convencionais para networks e o nascimento de uma nova economia*. São Paulo: Makron Books, 2001. p. 93.

no acesso a serviços, em detrimento da propriedade de bens físicos. Empresas agora oferecem plataformas e serviços digitais, transformando a forma como os consumidores se relacionam com o mercado.

A transição para uma economia de acesso impacta não só as práticas comerciais, mas também os princípios constitucionais da ordem econômica, que buscam equilibrar desenvolvimento econômico com justiça social e proteção do consumidor. A Constituição brasileira estabelece diretrizes que orientam a atividade econômica, como a defesa da concorrência e a função social da propriedade. No entanto, com a desmaterialização dos bens e a crescente centralidade dos serviços digitais, surgem novas formas de vulnerabilidade, especialmente relacionadas à proteção do consumidor. Nesse contexto, é essencial que o ordenamento jurídico acompanhe essas mudanças, garantindo a proteção dos direitos dos consumidores enquanto promove um ambiente econômico dinâmico e inovador, em conformidade com os princípios constitucionais.

Ademais, o desenvolvimento econômico impulsionado pelo comércio digital e pelas redes de acesso coloca novos desafios para a regulamentação, que precisa assegurar a transparência e a responsabilização das plataformas digitais. As práticas comerciais na sociedade em rede exigem uma abordagem que combine inovação com responsabilidade, promovendo um crescimento econômico sustentável e inclusivo. Isso se alinha com os princípios da ordem econômica que visam preservar o equilíbrio entre o crescimento econômico e os direitos fundamentais, como a dignidade da pessoa humana e a proteção do consumidor. Dessa forma, o marco regulatório do comércio eletrônico deve considerar as particularidades do ambiente digital e fornece diretrizes claras para que a economia de acesso possa florescer de maneira equitativa e responsável.

A economia digital, impulsionada pela sociedade de redes, não se baseia mais na posse de bens, mas no acesso contínuo a serviços e funcionalidades digitais. Esse modelo altera profundamente as dinâmicas comerciais tradicionais, exigindo uma abordagem legal que assegure transparência e responsabilidade das plataformas digitais, especialmente considerando a natureza imaterial e onipresente do comércio digital atual.

Essa transição para a era do acesso não apenas altera as práticas comerciais, mas também influencia profundamente as relações sociais e a dinâmica de poder entre produtores e consumidores. Rifkin destaca que, à medida que o acesso se torna

uma nova medida de valor nas interações sociais e comerciais, a noção de propriedade privada começa a perder sua centralidade. Essa nova lógica redefine os direitos e as responsabilidades dos consumidores, que passam a depender mais do acesso contínuo a serviços do que da posse permanente de bens.⁴⁷

Além disso, nas comunidades planejadas baseadas no acesso, como as descritas nos Estados Unidos, a vida se organiza em torno da troca de serviços e do uso compartilhado de espaços, o que redefine a noção de propriedade. Nesses espaços, os residentes têm menos controle sobre suas propriedades físicas, mas têm acesso garantido a uma ampla gama de serviços e experiências.⁴⁸ Essa tendência reflete uma mudança mais ampla na economia global, onde o valor está cada vez mais atrelado à capacidade de acessar recursos, em vez de à posse material.

O comércio na era digital intensifica ainda mais essa tendência de desmaterialização, uma vez que o comércio eletrônico e os serviços baseados em plataformas digitais são construídos em torno do conceito de acesso imediato e contínuo.⁴⁹ O consumidor pós-moderno, nesse cenário, torna-se um usuário de serviços digitais, que paga pelo acesso a experiências e funcionalidades, em vez de adquirir bens de forma tradicional. Isso traz novos desafios, como a necessidade de regulação e proteção de direitos em um ambiente onde a propriedade é substituída pela simples permissão de acesso.

Com o avanço da tecnologia e a digitalização das relações econômicas, o século XXI inaugurou um novo capítulo na história do comércio: o comércio eletrônico. Esse modelo de negócios se consolidou rapidamente, transformando a forma como produtos e serviços são ofertados e consumidos. Através da *internet*, empresas e consumidores podem realizar transações de maneira eficiente e sem barreiras geográficas, expandindo significativamente o alcance do mercado. Esse fenômeno contemporâneo é o resultado de séculos de evolução econômica, que começou com a subsistência, passou pelo escambo, desenvolvimento do comércio tradicional e agora se manifesta de forma digital, promovendo um novo nível de interatividade e dinamismo econômico.

⁴⁷ RIFKIN, Jeremy. *A era do acesso: a transição de mercados convencionais para networks e o nascimento de uma nova economia*. São Paulo: Makron Books, 2001. p. 94.

⁴⁸ RIFKIN, Jeremy. *A era do acesso: a transição de mercados convencionais para networks e o nascimento de uma nova economia*. São Paulo: Makron Books, 2001. 95.

⁴⁹ RIFKIN, Jeremy. *A era do acesso: a transição de mercados convencionais para networks e o nascimento de uma nova economia*. São Paulo: Makron Books, 2001. 96.

O comércio eletrônico envolve a troca voluntária de produtos ou serviços e, apesar de recente na sociedade, ganhou força rapidamente com o avanço tecnológico. A disseminação da *internet* trouxe inúmeras facilidades para fornecedores e consumidores, sendo a principal delas a possibilidade de realizar compras e vendas sem a necessidade de presença física. Nesse contexto, é perceptível o crescimento contínuo do *e-commerce*, acompanhado de seus prós e contras. Os consumidores desse tipo de mercado frequentemente se deparam com a simplicidade proporcionada pelo comércio eletrônico, mas também com a falta de confiança relacionada à troca e entrega das mercadorias adquiridas.

Leyser define o fenômeno do *e-commerce* como uma extensão do comércio tradicional, ocorrendo em um ambiente digital onde as transações de troca, compra, venda e prestação de serviços são realizadas com o apoio de equipamentos e softwares de informática, permitindo assim a negociação, a conclusão e até mesmo a execução do contrato, especialmente no caso de bens intangíveis.⁵⁰

Assim, o *e-commerce* pode ser entendido como transações realizadas por meio eletrônico de dados, conectados via *internet*. Nesse contexto, uma empresa cria um site que funciona como uma "vitrine *on-line*" para a exposição e venda de seus produtos. O *e-commerce* é fruto da tecnologia, representando uma nova forma de se realizar uma das atividades mais antigas da humanidade: o comércio. No entanto, a compra e venda *on-line* pode deixar o consumidor vulnerável, pois não há contato físico com o fornecedor, impossibilitando a verificação da veracidade da oferta anunciada.

O ambiente virtual trouxe facilidade ao consumidor, que pode realizar compras com um clique. Contudo, essa conveniência também pode levar a compras impulsivas, sem a devida pesquisa de mercado. Como resultado, o *e-commerce* se tornou alvo de muitas reclamações de consumidores que se sentem lesados, tornando-se fundamental determinar o aparato jurídico que rege essas relações, tema que será abordado nos próximos capítulos deste estudo.

O debate sobre a regulamentação do comércio eletrônico não é novo no sistema jurídico brasileiro. Neto *et al.* observa que "o comércio eletrônico no Brasil se expandiu em grande velocidade nos últimos anos e, conseqüentemente, os conflitos

⁵⁰ LEYSER, Maria Fátima Vaquero Ramalho. *O comércio eletrônico e o Código de Defesa do Consumidor*. Consultor Jurídico, 24 de maio de 2021. Disponível em: <https://www.conjur.com.br/2021-mai-24/mp-debate-comercio-eletronico-codigo-defesa-consumidor/>. Acesso em: 07 jul. 2024.

entre fornecedores e consumidores aumentaram na mesma proporção”.⁵¹

No *e-commerce*, as transações comerciais são definidas pela posição jurídica dos envolvidos: Business to Consumer (B2C) e Consumer to Consumer (C2C). A B2C envolve transações entre uma empresa e um consumidor, enquanto a C2C ocorre entre consumidores, sem a atuação do Código de Defesa do Consumidor, regulada pelo Código Civil de 2002, sendo uma relação de igual para igual, pois não há a presença de um fornecedor.⁵²

Nesse contexto, Maceira *et al.* afirma que o comércio eletrônico abrange qualquer tipo de negócio ou transação comercial que envolva a transferência de informações via *internet*. Existem diferentes modelos de negócios estabelecidos pelo *e-commerce*, como o B2B (*Business to Business*) e o B2C (*Business to Consumer*), este último direcionado diretamente ao consumidor. O B2C está em rápido crescimento em diversas áreas de bens e serviços, acompanhado pela proliferação de lojas *on-line*.⁵³

O B2B (*Business to Business*) é uma categoria que movimenta considerável quantia de dinheiro no Brasil e apresenta grande potencial de expansão. Essa modalidade ocorre quando uma organização comercializa seus produtos para outras empresas. Diferentemente do B2C (*Business to Consumer*), o B2B envolve transações comerciais entre empresas, geralmente realizadas através de plataformas de comércio eletrônico.⁵⁴

O comércio eletrônico, de fato, representa um fenômeno significativo na área empresarial, trazendo inúmeros benefícios para a economia do país, e deve ser continuamente incentivado. No entanto, os consumidores ainda enfrentam algumas barreiras devido à forma como os negócios são conduzidos *on-line*, como sua vulnerabilidade, que será abordada no decorrer do estudo.

A evolução tecnológica, embora tenha ampliado o acesso a produtos e serviços, também aumentou a insegurança e a vulnerabilidade. Isso se deve ao fato de que os contratos eletrônicos carecem da presença física característica dos

⁵¹ NETO, José Luiz Castro et al. *Comércio eletrônico: análise dos fatores críticos*. Business Review, v. 9, p. 1-25, 2010. p. 12.

⁵² CARDOSO, Simone; KAWAMOTO, Márcia Hiroko; MASSUDA, Ely Mitie. *Comércio eletrônico: o varejo virtual brasileiro*. Revista Cesumar–Ciências Humanas e Sociais Aplicadas, v. 24, n. 1, p. 117-134, 2019.

⁵³ SCANDIUZZI, Fernando. *Negócio eletrônico: a logística no comércio eletrônico business to consumer (B2C) em empresas nacionais*. 2005. Tese de Doutorado. Universidade de São Paulo. 2005. p. 14.

⁵⁴ SCANDIUZZI, Fernando. *Negócio eletrônico: a logística no comércio eletrônico business to consumer (B2C) em empresas nacionais*. 2005. Tese de Doutorado. Universidade de São Paulo. 2005. p. 14.

contratos tradicionais, gerando várias dúvidas e inseguranças. Problemas comuns incluem falta de informações sobre o produto, dificuldade em identificar o fornecedor, atrasos na entrega, e não recebimento do produto, entre outros.

À medida que o comércio eletrônico continua a crescer e se consolidar, é essencial que o aparato jurídico evolua para proteger os consumidores contra possíveis abusos e fraudes. A ausência de contato físico e a confiança nas plataformas digitais aumentam a necessidade de regulamentações específicas que assegurem a transparência e a responsabilidade dos fornecedores. A proteção do consumidor *on-line* deve ser reforçada para mitigar riscos associados a algoritmos opacos e práticas comerciais enganosas. Portanto, a adaptação das leis e a criação de mecanismos de proteção são fundamentais para garantir um ambiente comercial seguro e justo, onde os direitos dos consumidores sejam efetivamente preservados e respeitados.

A internet tem transformado profundamente a forma como os consumidores acessam e utilizam produtos e serviços. Inicialmente, serviços bancários e a compra de produtos que antes exigiam presença física passaram a ser realizados online, oferecendo aos consumidores praticidade e economia de tempo. Além disso, a internet permite encontrar fornecedores que melhor atendem às necessidades dos consumidores, com informações detalhadas sobre características e preços dos produtos, facilitando a comparação entre diferentes opções sem interação direta com vendedores, o que representa uma vantagem significativa do comércio digital.⁵⁵

A facilidade de contratação online, incluindo contratos de “um clique” e meios de pagamento simplificados, ilustra como o comércio digital se distingue pela agilidade e segurança percebida nos métodos de pagamento. Essa conveniência, no entanto, levanta a questão da confiança do consumidor no produto oferecido e na precisão da entrega, aspectos que precisam de regulamentação para manter a confiança do consumidor no ambiente digital.⁵⁶

No ambiente digital, surgem novas formas de intermediação entre fornecedores e consumidores, como o fornecimento de produtos por meio de plataformas digitais, que organizam e aproximam os interessados, otimizando o processo de compra e

⁵⁵ MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. Revista de Direito do Consumidor, São Paulo, vol. 125, p. 1-16, set.-out. 2019. p. 2.

⁵⁶ MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. Revista de Direito do Consumidor, São Paulo, vol. 125, p. 1-16, set.-out. 2019. p. 2.

reduzindo custos operacionais. Essa intermediação facilita a identificação de produtos e serviços adequados às necessidades dos consumidores e apresenta um modelo de negócios que favorece a acessibilidade e eficiência.⁵⁷

O advento da internet das coisas (IoT) e da inteligência artificial impactou as relações de consumo, permitindo a automatização e personalização de produtos com base em dados do consumidor, o que traz vantagens em termos de eficiência e agilidade. No entanto, esses avanços também aumentam os riscos associados a defeitos de software e a potencial dependência dos consumidores dos fornecedores, que podem influenciar a durabilidade e a funcionalidade dos produtos adquiridos.⁵⁸

Com o aumento do uso da internet via dispositivos móveis, o consumidor mantém-se conectado continuamente, o que facilita o rastreamento e armazenamento de suas atividades. Esse cenário expõe o consumidor a uma falta de controle sobre quais dados estão sendo utilizados e compartilhados no mercado da informação, destacando a necessidade de proteção reforçada para garantir privacidade e segurança no ambiente digital.⁵⁹

O ambiente virtual promove uma nova forma de isolamento, em que o usuário se encontra permanentemente conectado, tornando-se mais suscetível a influências externas. Essa conectividade ininterrupta possibilita um contato direto e intenso entre empresas e consumidores, inundando o usuário com mensagens publicitárias em diversas plataformas, como e-mails, Facebook e YouTube, o que intensifica o consumo sem intermediários.⁶⁰

Portanto, para proteger o consumidor nesse ambiente desmaterializado, os fornecedores têm o dever de fornecer informações claras e completas durante a contratação online, especialmente em relação aos contratos existenciais, que visam atender necessidades essenciais do consumidor, baseando-se nos princípios da

⁵⁷ MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. *Revista de Direito do Consumidor*, São Paulo, vol. 125, p. 1-16, set.-out. 2019. p. 7.

⁵⁸ MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. *Revista de Direito do Consumidor*, São Paulo, vol. 125, p. 1-16, set.-out. 2019. p. 3.

⁵⁹ MARTINS, Guilherme Magalhães. *Contratos eletrônicos de compra na internet e a proteção do consumidor*. Consultor Jurídico, São Paulo, 26 abr. 2017. Disponível em: <https://www.conjur.com.br/2017-abr-26/garantias-consumo-contratos-eletronicos-internet-protecao-consumidor>. Acesso em: 11 nov. 2024.

⁶⁰ MARTINS, Guilherme Magalhães. *Contratos eletrônicos de compra na internet e a proteção do consumidor*. Consultor Jurídico, São Paulo, 26 abr. 2017. Disponível em: <https://www.conjur.com.br/2017-abr-26/garantias-consumo-contratos-eletronicos-internet-protecao-consumidor>. Acesso em: 11 nov. 2024.

dignidade e solidariedade social, previstos na Constituição Federal.⁶¹

1.2.1 Novos produtos

O artigo 3º, §1º do Código de Defesa do Consumidor (CDC) definiu o termo "produto" de forma moderna e apropriada, preferindo esse termo em vez de "bem" ou "coisa".⁶² Baseando-se nesse artigo, Gama explica que, nas relações de consumo, um produto é qualquer bem que pode ser “móvel ou imóvel, material ou imaterial, desde que tenha valor econômico”.⁶³

Segundo Nunes, o conceito de produto é universal atualmente e está intimamente ligado à ideia de bem, resultante da produção no mercado de consumo das sociedades capitalistas contemporâneas.⁶⁴ É vantajoso seu uso, pois o conceito tem validade no meio jurídico e já era usado por todos os outros agentes do mercado (econômico, financeiro, de comunicações etc.). Adicionalmente, Filomeno esclarece em sua obra que, apesar de o termo "bem" ter sido substituído por "produto", o primeiro ainda é utilizado atualmente, indicando que "bem" possui um significado mais amplo do que "produto".⁶⁵

Com o avanço da *internet* e das tecnologias digitais, o comércio eletrônico transformou significativamente a forma como produtos são comercializados. No contexto do comércio eletrônico, o conceito de "produto" se amplia para incluir tanto bens tangíveis quanto intangíveis, englobando uma vasta gama de itens que podem ser adquiridos *on-line*. Esta concepção moderna de produto é essencial para entender o impacto e o desenvolvimento do comércio eletrônico na economia contemporânea.

O comércio eletrônico permite que os consumidores realizem compras a qualquer hora e de qualquer lugar, proporcionando uma conveniência sem precedentes. Segundo Santos *et al.*, essa flexibilidade é um dos principais atrativos

⁶¹ MARTINS, Guilherme Magalhães. Contratos eletrônicos de compra na internet e a proteção do consumidor. Consultor Jurídico, São Paulo, 26 abr. 2017. Disponível em: <https://www.conjur.com.br/2017-abr-26/garantias-consumo-contratos-eletronicos-internet-protecao-consumidor>. Acesso em: 11 nov. 2024.

⁶² BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 30 jun. 2024.

⁶³ GAMA, Hélio Zaghetto. *Curso de Direito do Consumidor*. 1ª Ed – 4ª tiragem. Rio de Janeiro: Forense, 2002. p. 29.

⁶⁴ NUNES, Rizzatto. *Curso de Direito do Consumidor*, 12ª Edição. Editora Saraiva, 2018.

⁶⁵ FILOMENO, José Geraldo Brito. *Manual de Direitos do Consumidor*. 5. ed. rev., atual. e ref. – São Paulo: Atlas, 2018.

do *e-commerce*, que elimina a necessidade de deslocamento físico e permite acesso contínuo a uma vasta gama de produtos e serviços. Este acesso facilitado impulsiona a competitividade entre as empresas, forçando-as a inovar constantemente para atrair e manter clientes.⁶⁶

Além da conveniência, o *e-commerce* oferece uma plataforma para a personalização e a segmentação de mercado. Utilizando tecnologias de análise de dados e inteligência artificial, as empresas podem criar experiências de compra personalizadas, ajustadas às preferências e comportamentos dos consumidores. Isso não só melhora a satisfação do cliente, mas também aumenta a fidelização e as taxas de conversão de vendas.

O impacto do comércio eletrônico no setor varejista é particularmente notável. Conforme observado por Gama, as empresas varejistas têm adaptado suas estratégias para incluir plataformas *on-line* como uma extensão natural de seus negócios físicos. Esta integração permite que os varejistas alcancem um público mais amplo, melhorem a eficiência operacional e reduzam custos associados à manutenção de lojas físicas.⁶⁷

A utilização de plataformas de *e-commerce* também facilita a gestão de logística. Com sistemas integrados, os varejistas podem monitorar em tempo real o *status* de estoque, prever demandas e otimizar processos de reabastecimento. Essa eficiência operacional resulta em menor desperdício e maior capacidade de atender rapidamente às necessidades dos clientes.⁶⁸

No entanto, o comércio eletrônico não está isento de desafios. A segurança nas transações *on-line* continua sendo uma preocupação significativa, tanto para consumidores quanto para empresas. Segundo Moreira, a implementação de medidas robustas de segurança cibernética é crucial para proteger dados sensíveis e garantir a confiança do consumidor. Sem essa confiança, a adoção do *e-commerce* pode ser prejudicada.⁶⁹

Outro desafio relevante é a logística de entrega. O aumento das compras *on-line* demanda uma infraestrutura eficiente para a entrega de produtos. Fatores como

⁶⁶ SANTOS, E. B. dos; et al. *Marketing na Era Digital*. VI Jornada Acadêmica: Goiás, 2012.

⁶⁷ GAMA, Hélio Zaghetto. *Curso de Direito do Consumidor*. 1ª Ed – 4ª tiragem. Rio de Janeiro: Forense, 2002.

⁶⁸ GAMA, Hélio Zaghetto. *Curso de Direito do Consumidor*. 1ª Ed – 4ª tiragem. Rio de Janeiro: Forense, 2002.

⁶⁹ MOREIRA, R. A. *O Comércio Eletrônico, Os Métodos de Pagamentos e os Mecanismos de Segurança*. FATEC: Jahu, 2016.

a rapidez na entrega, a rastreabilidade e o custo do frete são determinantes para a satisfação do cliente e, conseqüentemente, para o sucesso do comércio eletrônico. Conforme apontado por Claro, soluções inovadoras em logística, como centros de distribuição automatizados e parcerias com serviços de entrega, são essenciais para superar esses obstáculos.⁷⁰

A pandemia de COVID-19 acelerou a adoção do comércio eletrônico, com um aumento substancial no número de consumidores recorrendo às compras *on-line*.⁷¹ Essa mudança forçou muitas empresas a digitalizar suas operações rapidamente, adotando novas tecnologias para manter a continuidade dos negócios e atender à crescente demanda do comércio eletrônico.

Além dos benefícios diretos, o *e-commerce* contribui para o desenvolvimento econômico mais amplo, facilitando o acesso ao mercado para pequenas e médias empresas (PMEs). O comércio eletrônico elimina muitas das barreiras tradicionais à entrada no mercado, permitindo que essas empresas alcancem clientes em uma escala global. Este aspecto democratiza o comércio, promovendo uma competição mais justa e incentivando a inovação.⁷²

Em termos de *marketing*, o comércio eletrônico oferece ferramentas poderosas para a promoção e a comunicação com os clientes. Plataformas de mídia social, campanhas de *e-mail marketing* e anúncios segmentados são alguns dos métodos utilizados pelas empresas para engajar consumidores e promover produtos. Conforme observado por Nanehkaran, essas estratégias não apenas aumentam a visibilidade da marca, mas também permitem uma interação mais direta e personalizada com os clientes.⁷³

O futuro do comércio eletrônico parece promissor, com expectativas de crescimento contínuo e evolução tecnológica. A integração de tecnologias emergentes, como a realidade aumentada e virtual, promete transformar ainda mais a experiência de compra *on-line*, tornando-a mais interativa e envolvente.⁷⁴ A

⁷⁰ CLARO, Alberto Carvalho dos Santos. *Comércio Eletrônico*. 1ª Edição: São Paulo, 2013.

⁷¹ SEBRAE. *Crescimento do e-commerce na pandemia é fruto de investimentos e muito trabalho*. Disponível em: <https://sebraepr.com.br/comunidade/artigo/crescimento-do-e-commerce-na-pandemia-e-fruto-de-investimentos-e-muito-trabalho>. Acesso em: 01 ago. 2024.

⁷² NANEHKARAN, Y. A. *An introduction to electronic commerce*. International Journal of Scientific & Technology Research, v. 2, n. 4, p. 190-193, 2013.

⁷³ NANEHKARAN, Y. A. *An introduction to electronic commerce*. International Journal of Scientific & Technology Research, v. 2, n. 4, p. 190-193, 2013.

⁷⁴ SOLOMON, M. R. *O Comportamento do Consumidor: comprando, possuindo e sendo*. 11. ed. Porto Alegre: Bookman, 2016.

evolução constante do *e-commerce* continuará a moldar o cenário econômico global, apresentando novas oportunidades e desafios para empresas e consumidores.

A concepção de produto no comércio eletrônico é dinâmica e abrangente, refletindo as mudanças rápidas na tecnologia e nas preferências do consumidor. As vantagens proporcionadas pelo *e-commerce*, como conveniência, personalização e eficiência operacional, superam os desafios, fazendo dele uma ferramenta essencial para o desenvolvimento do comércio e para a economia global.⁷⁵

O comércio eletrônico tem se mostrado uma ferramenta essencial para o desenvolvimento do comércio moderno, oferecendo uma definição ampla de produtos, que inclui tanto bens físicos quanto digitais. No entanto, com o crescimento desse mercado, é fundamental abordar as questões de proteção do consumidor *on-line*. O avanço do *e-commerce* traz conveniência e inovação, mas também apresenta novos riscos, especialmente relacionados à vulnerabilidade algorítmica e digital.

É válido ressaltar que o comércio eletrônico tem desempenhado um papel significativo na democratização do acesso aos mercados, permitindo que consumidores e pequenos empreendedores participem de transações comerciais de forma mais ampla e inclusiva. A redução dos custos de busca e a facilidade de comparação de preços e produtos online ampliaram as opções disponíveis aos consumidores, promovendo uma maior competitividade entre os fornecedores. Além disso, plataformas digitais têm possibilitado que pequenos negócios alcancem mercados antes inacessíveis, contribuindo para a diversificação econômica e a inclusão de novos atores no cenário comercial.⁷⁶

No entanto, apesar desses avanços, o comércio eletrônico também pode perpetuar ou até mesmo ampliar exclusões no acesso aos mercados. A falta de infraestrutura tecnológica adequada e a ausência de habilidades digitais em determinadas regiões ou grupos populacionais podem limitar a participação plena no ambiente digital. Essa exclusão digital resulta em barreiras significativas para consumidores e empreendedores que não conseguem se adaptar às novas exigências do mercado eletrônico, perpetuando desigualdades socioeconômicas.⁷⁷

⁷⁵ SOLOMON, M. R. *O Comportamento do Consumidor: comprando, possuindo e sendo*. 11. ed. Porto Alegre: Bookman, 2016.

⁷⁶ BAKOS, Yannis. *Reducing buyer search costs: implications for electronic marketplaces*. Management Science, v. 43, n. 12, 1997. p. 3.

⁷⁷ BONILLA, Maria Helena. *Inclusão digital: polêmica contemporânea*. In: PRETTO, Nelson de Luca; BONILLA, Maria Helena (Orgs.). *Inclusão digital: polêmica contemporânea*. Salvador: Edufba, 2005. p. 51.

Do ponto de vista jurídico, é essencial que as políticas públicas abordem essas disparidades, promovendo a inclusão digital e garantindo que os benefícios do comércio eletrônico sejam acessíveis a todos. A implementação de programas de capacitação tecnológica e a expansão da infraestrutura de internet são medidas fundamentais para assegurar que indivíduos e empresas possam participar efetivamente do mercado digital. Além disso, a criação de regulamentações que protejam os direitos dos consumidores e promovam a concorrência leal é essencial para evitar práticas discriminatórias e assegurar um ambiente de negócios equitativo.⁷⁸

Em suma, enquanto o comércio eletrônico oferece oportunidades significativas para a democratização do acesso aos mercados, é imperativo reconhecer e abordar os desafios que podem levar à exclusão de determinados grupos. A adoção de políticas inclusivas e a promoção de uma infraestrutura tecnológica acessível são passos essenciais para garantir que os benefícios do comércio eletrônico sejam distribuídos de maneira equitativa, contribuindo para a redução das desigualdades e o fortalecimento da economia digital.

Portanto, é fundamental que a proteção ao consumidor seja plenamente respeitada para minimizar esses riscos e garantir que os benefícios do comércio eletrônico sejam aproveitados de maneira justa e segura por todos. Isso ressalta a importância de equilibrar a inovação tecnológica com medidas de segurança, promovendo um ambiente digital confiável para consumidores e empresas.

1.2.2 Novos serviços

O conceito de serviço está especificado no artigo 3º, §2º do Código de Defesa do Consumidor (CDC), onde é descrito como qualquer atividade disponibilizada no mercado mediante remuneração, incluindo serviços bancários, de crédito, financeiros e securitários, com exceção dos serviços de caráter trabalhista.⁷⁹ Isso demonstra que o CDC utiliza a palavra "qualquer" de maneira exemplificativa, indicando que o serviço engloba qualquer atividade oferecida no mercado de consumo, não se limitando às

⁷⁸ SILVEIRA, Sérgio Amadeu. A noção de exclusão digital diante das exigências de uma cibercidadania. In: HETKOWSKI, Tânia Maria (Org.). Políticas públicas & inclusão digital. Salvador: EDUFBA, 2008. p. 60.

⁷⁹ BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 30 jun. 2024.

modalidades listadas no Código.⁸⁰

Gama, em sua obra, comenta a definição de serviço adotada pelo CDC, descrevendo-o como uma atividade remunerada, mesmo que seja de natureza financeira, bancária, de crédito ou securitária. O CDC define como Serviço a atividade remunerada, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista. Importante é que seja atividade exercida com certa repetição e sempre em caráter remunerado. Algumas atividades gratuitas, fornecidas graciosamente no bojo das demais ofertas de bens e serviços, não perdem o caráter de serviço remunerado, pois há sempre embutido um interesse negocial.⁸¹

Filomeno compartilha dessa visão, afirmando que o Código de Defesa do Consumidor abrange todo e qualquer tipo de serviço, definido como uma utilidade oferecida ao consumidor por um fornecedor específico, configurando um "*facere*" (fazer).⁸²

O conceito de prestação de serviços no comércio eletrônico representa uma transformação significativa na maneira como os serviços são oferecidos e consumidos. Com a *internet*, os serviços podem ser disponibilizados de forma instantânea e global, eliminando a necessidade de interação física entre prestador e cliente. Nakamura define o comércio eletrônico como qualquer atividade de compra e venda realizada por meios eletrônicos, o que inclui uma ampla gama de serviços que agora podem ser acessados *on-line*.⁸³

A digitalização dos serviços permite uma maior personalização e conveniência para o consumidor. Serviços financeiros, bancários, de crédito e seguros, por exemplo, podem ser gerenciados inteiramente *on-line*, proporcionando aos clientes a possibilidade de realizar transações, consultar saldos, contratar seguros e obter créditos sem precisar sair de casa. Esse nível de conveniência é um dos principais atrativos do comércio eletrônico, conforme discutido por Kotler.⁸⁴

No contexto do comércio eletrônico, a prestação de serviços também facilita a criação de plataformas de intermediação, como *marketplaces* e aplicativos de entrega,

⁸⁰ NUNES, Rizzatto. *Curso de Direito do Consumidor*, 12ª Edição. Editora Saraiva, 2018.

⁸¹ GAMA, Hélio Zaghetto. *Curso de Direito do Consumidor*. 1ª Ed – 4ª tiragem. Rio de Janeiro: Forense, 2002.

⁸² FILOMENO, José Geraldo Brito. *Manual de Direitos do Consumidor*. 5. ed. rev., atual. e ref. – São Paulo: Atlas, 2018.

⁸³ NAKAMURA, R. R. *E-Commerce na Internet: Fácil de Entender*. São Paulo: Érica, 2001.

⁸⁴ KOTLER, P. *Administração de Marketing*. 10. ed. São Paulo: Prentice Hall Brasil, 2000.

que conectam prestadores de serviços e consumidores de maneira eficiente. Essas plataformas utilizam algoritmos avançados para personalizar ofertas e melhorar a experiência do usuário, aumentando a satisfação do cliente e a fidelidade à marca. O'Brien destaca que essas interações digitais tornam-se essenciais para a competitividade das empresas no mercado moderno.⁸⁵

No entanto, a prestação de serviços no comércio eletrônico também enfrenta desafios específicos. A falta de contato físico pode gerar desconfiança nos consumidores, especialmente em serviços que tradicionalmente dependem de interações presenciais. Além disso, questões relacionadas à segurança de dados e privacidade são críticas, uma vez que a maioria das transações de serviços *on-line* envolve o compartilhamento de informações pessoais sensíveis. Moura e Albertin apontam que garantir a segurança e a privacidade no ambiente digital é fundamental para ganhar a confiança dos consumidores.⁸⁶

Para mitigar esses desafios, as empresas de comércio eletrônico investem significativamente em tecnologias de segurança e protocolos de privacidade. Além disso, estratégias de atendimento ao cliente, como *chatbots* e suporte ao vivo, são implementadas para replicar a assistência personalizada que seria oferecida em um ambiente físico. Segundo Fleury, a formação de equipes qualificadas e bem treinadas para operar nesses ambientes digitais é crucial para garantir a qualidade dos serviços prestados.⁸⁷

Assim, os serviços no comércio eletrônico representam uma evolução significativa na maneira como as empresas interagem com os consumidores. Apesar dos desafios, os benefícios em termos de conveniência, alcance e eficiência são substanciais. A contínua pesquisa e inovação nesse campo são essenciais para explorar todo o potencial do comércio eletrônico e assegurar que tanto consumidores quanto empresas possam aproveitar ao máximo essas novas oportunidades.

Portanto, é essencial que a expansão dos serviços no comércio eletrônico venha acompanhada de fortes medidas de proteção ao consumidor, especialmente diante das vulnerabilidades no ambiente digital. A confiança do consumidor é

⁸⁵ O'BRIEN, J. A. *Sistemas de informação: e as decisões gerenciais na era da Internet*. 2. ed. São Paulo: Saraiva, 2004.

⁸⁶ MOURA, R. M.; ALBERTIN, A. L. *Comércio eletrônico: seus aspectos de segurança e privacidade*. Revista de Administração de Empresas, vol. 38, n. 2, 1998. Disponível em: https://rae.fgv.br/sites/rae.fgv.br/files/artigos/10.1590_S0034-901998000200006.pdf. Acesso em: 02 jul. 2024.

⁸⁷ FLEURY, M. T. L. *As pessoas na organização*. São Paulo: Editora Gente, 2002.

fundamental para o sucesso contínuo do *e-commerce*, e isso só pode ser alcançado através da garantia de segurança de dados e privacidade. Implementar regulamentações claras e tecnologias de segurança avançadas é essencial para proteger os consumidores contra fraudes e uso indevido de dados e informações pessoais. Ao fazer isso, não só se fortalece a confiança no comércio eletrônico, mas também se assegura que os benefícios da digitalização sejam plenamente aproveitados, proporcionando uma experiência segura e satisfatória para todos os envolvidos na relação consumerista.

1.3 A VULNERABILIDADE DO CONSUMIDOR NO COMÉRCIO ELETRÔNICO

A vulnerabilidade na relação de consumo é um aspecto fundamental que reflete a posição de desvantagem do consumidor frente ao fornecedor, sendo amplamente reconhecida no Código de Defesa do Consumidor (CDC). Essa fragilidade decorre de fatores como a assimetria de informações, a dependência econômica e a falta de conhecimento técnico por parte do consumidor, exigindo a intervenção do direito para garantir o equilíbrio e a justiça nas relações comerciais. Com o avanço tecnológico e a digitalização das relações de consumo, essa vulnerabilidade ganhou contornos mais complexos, demandando uma análise aprofundada dos desafios que surgem no ambiente digital.

Neste sentido, o presente tópico abordará três formas principais de vulnerabilidade no contexto do comércio eletrônico: a vulnerabilidade digital, a vulnerabilidade algorítmica e a vulnerabilidade na proteção de dados. Essas dimensões evidenciam como o ambiente virtual amplia os riscos enfrentados pelos consumidores, especialmente em razão da opacidade das práticas tecnológicas e da falta de transparência na coleta e uso de dados pessoais. Dessa forma, será apresentada uma reflexão sobre como essas vulnerabilidades afetam os consumidores no comércio eletrônico, destacando a importância de medidas que assegurem a proteção de seus direitos. A análise buscará evidenciar a necessidade de um arcabouço regulatório mais robusto e adaptado às especificidades do ambiente digital, com o objetivo de garantir relações comerciais justas e seguras.

1.3.1 Vulnerabilidade digital

O princípio da vulnerabilidade é um dos pilares fundamentais do Código de Defesa do Consumidor (CDC), refletindo a necessidade de proteção diferenciada do consumidor nas relações de consumo. Previsto no artigo 4º, inciso I, do CDC, esse princípio reconhece que o consumidor é a parte mais fraca na relação com o fornecedor, seja por uma inferioridade técnica, jurídica ou econômica.⁸⁸ Essa vulnerabilidade, conforme argumenta Miragem, é intrínseca à posição do consumidor e justifica a intervenção do direito para reequilibrar as relações de consumo, promovendo a isonomia e a justiça nas interações comerciais.⁸⁹

Com a evolução das tecnologias e a crescente digitalização das relações de consumo, essa vulnerabilidade tradicional ganhou novas dimensões. No ambiente digital, a vulnerabilidade informacional se torna ainda mais pronunciada, uma vez que os consumidores enfrentam desafios adicionais, como a complexidade dos algoritmos, a opacidade das políticas de privacidade, e a falta de transparência nas práticas de coleta e uso de dados pessoais. Esses fatores ampliam a vulnerabilidade do consumidor, que se vê cada vez mais exposto a riscos de manipulação e exploração no ciberespaço.

A vulnerabilidade digital do consumidor se intensifica à medida que as interações sociais e comerciais migram para o ambiente virtual. Essa vulnerabilidade decorre não apenas da falta de conhecimento técnico por parte dos consumidores, mas também das práticas estruturais e sistêmicas que exploram essa fragilidade. No contexto digital, as vulnerabilidades tradicionais do consumidor são amplificadas devido à opacidade dos algoritmos e à manipulação de dados pessoais, criando um ambiente onde o consumidor se torna mais suscetível a práticas abusivas.⁹⁰

A vulnerabilidade informacional é exacerbada no ambiente digital. O consumidor, frequentemente, não dispõe de informações suficientes sobre seus direitos ou sobre os produtos e serviços que adquire, o que o coloca em uma posição de desvantagem nas relações de consumo. Essa assimetria informacional é explorada pelas empresas, que utilizam os dados coletados para segmentar e direcionar ofertas,

⁸⁸ BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 30 jun. 2024.

⁸⁹ MIRAGEM, Bruno. *Curso de Direito do Consumidor*. 8. ed. São Paulo: Revista dos Tribunais, 2020.

⁹⁰ MARQUES, Claudia Lima; MUCELIN, Guilherme. *A vulnerabilidade digital do consumidor no ciberespaço: novas perspectivas para a proteção de dados pessoais e o papel do direito do consumidor*. Revista de Direito do Consumidor, São Paulo, v. 134, p. 15-38, jan./fev. 2022.

muitas vezes sem o devido consentimento informado do consumidor.⁹¹

No ambiente digital, a vulnerabilidade técnica e jurídica também se destaca. A falta de conhecimento especializado dos consumidores sobre os produtos e serviços digitais, combinada com a complexidade dos termos de uso e políticas de privacidade, dificulta a proteção dos direitos do consumidor. Além disso, a falta de clareza e a complexidade desses documentos muitas vezes resultam em um consentimento mais aparente do que real, contribuindo para a perpetuação dessa vulnerabilidade.⁹²

Outro aspecto relevante é a vulnerabilidade estrutural causada pelo *design* das plataformas digitais, que muitas vezes é deliberadamente criado para manipular o comportamento do consumidor. A arquitetura digital de escolha visa antecipar e explorar preconceitos cognitivos e afetivos dos consumidores, o que pode resultar em decisões que não refletem seus reais interesses. Essa manipulação é especialmente problemática quando combinada com a coleta e tratamento intensivo de dados pessoais, criando um ciclo de vulnerabilidade que se perpetua no ambiente digital.⁹³

A dependência das plataformas digitais também contribui para a vulnerabilidade situacional dos consumidores. Essa dependência cria uma espécie de "catividade digital", onde os consumidores se veem obrigados a continuar utilizando determinados serviços, mesmo cientes dos riscos, devido à falta de alternativas viáveis. Essa situação é agravada pela falta de transparência sobre como os dados pessoais são utilizados, o que muitas vezes resulta em uma perda de controle sobre informações sensíveis.⁹⁴

Ademais, a discriminação algorítmica representa uma nova forma de vulnerabilidade digital, onde consumidores podem ser tratados de maneira desigual com base em perfis criados a partir de seus dados pessoais. Essa prática pode levar à exclusão ou estigmatização de determinados grupos de consumidores, exacerbando as desigualdades no acesso a bens e serviços no ambiente digital. Esse tipo de discriminação, ainda que muitas vezes legalmente justificável, fere princípios fundamentais de igualdade e não discriminação, exigindo uma resposta jurídica

⁹¹ BEHRENS, Yan West. *Comércio eletrônico de produtos e serviços: uma análise das principais práticas abusivas em prejuízo dos consumidores*. Salvador: Paginece, 2014.

⁹² MENDES, Laura Schertel. *A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais*. Revista de Direito do Consumidor, São Paulo, v. 102, p. 19-43, nov./dez. 2015.

⁹³ MICKLITZ, Hans-W.; HELBERGER, Natali; STRYCHARZ, Joanna et al. *EU consumer protection 2.0: Structural asymmetries in digital consumer markets*. Bruxelas: BEUC, mar. 2021.

⁹⁴ MARQUES, Claudia Lima; MUCELIN, Guilherme. *A vulnerabilidade digital do consumidor no ciberespaço: novas perspectivas para a proteção de dados pessoais e o papel do direito do consumidor*. Revista de Direito do Consumidor, São Paulo, v. 134, p. 15-38, jan./fev. 2022.

apropriada.⁹⁵

Finalmente, a complexidade e a ubiquidade dos dados na *internet* criam novas camadas de vulnerabilidade. O conceito de vulnerabilidade digital é dinâmico e se adapta à medida que a tecnologia evolui, exigindo que o direito do consumidor também evolua para proteger os consumidores nesse novo ambiente. Os dados pessoais são agora uma fonte de poder, e a falta de proteção adequada pode levar a violações significativas dos direitos fundamentais dos consumidores.⁹⁶

A vulnerabilidade digital do consumidor é uma questão complexa que exige uma abordagem abrangente e adaptativa para garantir a proteção dos consumidores no ambiente digital. As reflexões de Marques e Mucelin, juntamente com as contribuições de outros autores, fornecem uma base sólida para entender e enfrentar esses desafios, destacando a necessidade de uma maior transparência, responsabilidade e proteção dos direitos dos consumidores na era digital.

Quadro 1– Conceito de diversos autores sobre vulnerabilidade digital

Helberger et al. (2021)	Propuseram o conceito normativo de “assimetria digital” para descrever a vulnerabilidade estrutural dos consumidores na economia digital, destacando a incapacidade de proteção adequada pelos reguladores.
Hyde e Cartwright (2023)	Analisaram como a infraestrutura digital pode explorar a vulnerabilidade dos consumidores por meio de microtransações e padrões obscuros, expondo falhas regulatórias na proteção dos mais vulneráveis.
Cantero Gamito (2023)	Focou na vulnerabilidade digital de menores em plataformas como o TikTok, destacando a complexidade regulatória que impede a proteção eficaz e a aplicação de leis voltadas para a proteção infantil.
Durovic e Poon (2023)	Exploram a vulnerabilidade dos consumidores nas mídias sociais, onde os termos e condições de uso de plataformas como Meta e TikTok falham em proteger adequadamente os usuários devido a lacunas na legislação.
Riefa e Saintier (2020)	Conceituam vulnerabilidade do consumidor no mercado digital da UE, destacando as “assimetrias estruturais” que criam uma vulnerabilidade sistêmica, exacerbada pela falha na aplicação das regulamentações.
Laura Schertel Mendes (2020)	Discutiu a vulnerabilidade digital do consumidor quanto ao tratamento de dados pessoais, destacando os desafios na proteção da privacidade e a necessidade de uma abordagem mais rigorosa na legislação brasileira.

⁹⁵ MARQUES, Claudia Lima; MUCELIN, Guilherme. *A vulnerabilidade digital do consumidor no ciberespaço: novas perspectivas para a proteção de dados pessoais e o papel do direito do consumidor*. Revista de Direito do Consumidor, São Paulo, v. 134, p. 15-38, jan./fev. 2022.

⁹⁶ BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento*. Ed 2. Vol. único. Rio de Janeiro: Forense, 2020.

Martins e Lima (2020)	Exploraram a transição da vulnerabilidade digital para uma vulnerabilidade empresarial, analisando como as empresas também estão sujeitas a riscos digitais que afetam sua operação e relacionamento com consumidores.
Júlio Camargo de Azevedo (2021)	A vulnerabilidade digital pode ser conceituada como a condição de suscetibilidade a riscos nos ambientes cibernéticos, que promove o surgimento de desigualdades, desequilíbrios de poder, restrições ao exercício da cidadania, bem como violações à privacidade, intimidade e à capacidade de autodeterminação informativa.

Fonte: Autor (2024).

A vulnerabilidade digital, como delineado por diversos autores, revela-se uma característica inerente do ambiente digital contemporâneo, caracterizada por uma profunda assimetria de poder entre consumidores e plataformas digitais. Helberger *et al.* introduzem o conceito de “assimetria digital,” que aponta para uma vulnerabilidade estrutural dos consumidores em meio à economia digital. Essa vulnerabilidade é intensificada pela incapacidade dos reguladores em fornecer uma proteção adequada, evidenciando as limitações das estruturas regulatórias atuais.⁹⁷

Hyde e Cartwright ampliam essa discussão ao analisar como a infraestrutura digital pode explorar as vulnerabilidades dos consumidores, especialmente através de práticas como microtransações e padrões obscuros. Esses mecanismos não apenas exploram, mas também aprofundam as falhas regulatórias, expondo consumidores a riscos que eles podem não ser capazes de compreender completamente ou evitar.⁹⁸

Já Cantero Gamito foca sua análise na vulnerabilidade digital de menores, especialmente em plataformas como o TikTok. Ele ressalta a complexidade regulatória como um fator que dificulta a proteção eficaz dos jovens, sugerindo que as leis existentes muitas vezes não acompanham a rápida evolução tecnológica e os desafios associados à proteção de grupos mais vulneráveis.⁹⁹

Durovic e Poon, por sua vez, exploram como as mídias sociais agravam a vulnerabilidade digital dos consumidores, destacando as falhas nos termos e condições de uso de plataformas como Meta e TikTok. As lacunas na legislação permitem que essas plataformas operem sem proteger adequadamente seus

⁹⁷ HELBERGER, N.; LYNSKEY, O.; MICKLITZ, H.-W.; ROTT, P.; SAX, M.; STRYCHARZ, J. *EU Consumer Protection 2.0: Structured Asymmetries in Digital Consumer Markets*. BEUC, 2021.

⁹⁸ HYDE, R.; CARTWRIGHT, P. *Exploring Consumer Detriment in Immersive Gaming Technologies*. Journal of Consumer Policy, v. 46, p. 335-361, 2023.

⁹⁹ CANETRO GAMITO, M. *Do too many cooks spoil the broth? How EU law underenforcement allows TikTok's violations of minors' rights*. Journal of Consumer Policy, v. 46, p. 281-305, 2023.

usuários, reforçando a necessidade de uma revisão das regulamentações.¹⁰⁰

Riefa e Saintier conceituam a vulnerabilidade do consumidor no mercado digital da UE, destacando as “assimetrias estruturais” que criam uma vulnerabilidade sistêmica. Eles apontam que a falha na aplicação das regulamentações existentes exacerba essas assimetrias, resultando em uma proteção inadequada para os consumidores.¹⁰¹

A questão da hipervulnerabilidade e ultravulnerabilidade, como discutido por Mucelin e Silva, expande os conceitos de vulnerabilidade digital para incluir grupos que estão em uma posição de vulnerabilidade extrema ou complexa. A hipervulnerabilidade refere-se a uma condição na qual indivíduos ou grupos estão sujeitos a um conjunto de riscos que não apenas os tornam mais suscetíveis, mas que também são exacerbados por fatores como desigualdades preexistentes, deficiência ou menoridade.¹⁰²

O conceito de ultravulnerabilidade, por outro lado, vai além, apontando para situações em que a vulnerabilidade é tão intensa que ultrapassa as capacidades regulatórias tradicionais. Nesse contexto, a tecnologia não apenas expõe os indivíduos a novos riscos, mas também potencializa essas ameaças, criando cenários em que as estruturas legais e regulatórias existentes são inadequadas para proteger os direitos dos indivíduos.¹⁰³

Mucelin e Silva argumentam que a proteção contra ultravulnerabilidade exige a criação de novos direitos, como os neurodireitos, que buscam proteger a integridade mental e a autonomia cognitiva dos indivíduos em um cenário digital onde essas faculdades são constantemente ameaçadas.¹⁰⁴

Assim, ao considerar a hipervulnerabilidade e a ultravulnerabilidade dentro do contexto da vulnerabilidade digital, fica claro que as abordagens regulatórias tradicionais são insuficientes. A necessidade de uma nova legislação e de mecanismos de proteção mais robustos é evidente para garantir que os direitos dos

¹⁰⁰ DUROVIC, M.; POON, T. *Consumer Vulnerability, Digital Fairness, and the European Rules on Unfair Contract Terms: What Can Be Learnt from the Case Law Against TikTok and Meta?* Journal of Consumer Policy, v. 46, p. 361-375, 2023.

¹⁰¹ RIEFA, C.; SAINTIER, S. *Protecting Vulnerable Consumers in the Digital Single Market*. European Business Law Review, v. 33, p. 607-634, 2020.

¹⁰² MUCELIN, Guilherme; SILVA, Roberta Scalzilli. *Neurodireitos e ultravulnerabilidade*. Revista de Direito do Consumidor, v. 153, p. 225-256, maio/jun. 2024.

¹⁰³ MUCELIN, Guilherme; SILVA, Roberta Scalzilli. *Neurodireitos e ultravulnerabilidade*. Revista de Direito do Consumidor, v. 153, p. 225-256, maio/jun. 2024.

¹⁰⁴ MUCELIN, Guilherme; SILVA, Roberta Scalzilli. *Neurodireitos e ultravulnerabilidade*. Revista de Direito do Consumidor, v. 153, p. 225-256, maio/jun. 2024.

indivíduos sejam respeitados e protegidos, especialmente em um ambiente digital que evolui rapidamente e onde as ameaças à privacidade e à autodeterminação informativa são cada vez mais complexas e invasivas.¹⁰⁵

Ante ao exposto, vale aferir que no comércio eletrônico, a confiança entre as partes é essencial e está associada ao princípio da boa-fé, o qual deve ser protegido devido às características particulares desse meio, que demanda uma expectativa legítima de segurança e clareza nas informações para o consumidor. Segundo Claudia Lima Marques, a confiança deve ser um paradigma central, ajudando a adaptar as normas de proteção do consumidor às novas exigências do ambiente digital.¹⁰⁶

Essa confiança atua como um guia para a divisão dos riscos, agora aumentados pelo fácil acesso e pela comodidade proporcionados pela tecnologia. No entanto, a boa-fé objetiva é apenas uma base; ela se complementa com a chamada "Teoria da Aparência," que atribui legitimidade jurídica àquilo que aparenta ser confiável e seguro, fornecendo ao consumidor uma proteção adicional no âmbito virtual.¹⁰⁷

A confiança, enquanto princípio, foi inicialmente desenvolvida na Alemanha e visa assegurar as expectativas legítimas entre as partes em uma relação contratual. Ela protege os consumidores ao estabelecer que obrigações assumidas por ambas as partes, quando pautadas pela boa-fé, integram o conteúdo do contrato, oferecendo uma defesa contra expectativas frustradas.¹⁰⁸

Portanto, para atender a essa proteção, as normas contratuais também reforçam a segurança jurídica, que é mantida não só pela declaração explícita de intenções, mas também pela conduta e pelas obrigações implícitas. Assim, a confiança e a boa-fé juntas se tornam pilares essenciais para garantir um ambiente comercial digital seguro e justo.

1.3.2 Vulnerabilidade algorítmica

¹⁰⁵ MUCELIN, Guilherme; SILVA, Roberta Scalzilli. *Neurodireitos e ultravulnerabilidade*. Revista de Direito do Consumidor, v. 153, p. 225-256, maio/jun. 2024.

¹⁰⁶ MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*. São Paulo: Revista dos Tribunais, 2004. p. 40.

¹⁰⁷ MARQUES, Cláudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*. São Paulo: Revista dos Tribunais, 2004. p. 40.

¹⁰⁸ Op. cit. p. 41.

A sociedade do controle¹⁰⁹ é caracterizada pela manipulação e modulação das redes digitais, as quais se tornam ferramentas poderosas de influência e domínio sobre os indivíduos. Essas redes, alimentadas por sistemas algorítmicos sofisticados, são capazes de captar e processar grandes quantidades de dados pessoais, que são utilizados para moldar comportamentos e decisões de maneira quase invisível.¹¹⁰

As plataformas digitais atuam como intermediárias em quase todas as esferas da vida social, coletando dados de maneira contínua e automatizada. Essa coleta massiva de dados permite às corporações tecnológicas realizar previsões comportamentais e, mais que isso, influenciar ativamente as escolhas dos usuários. Assim, os indivíduos se tornam objetos de uma modulação comportamental que não apenas antecipa suas ações, mas também as direciona, reforçando a lógica do capitalismo de vigilância.¹¹¹

A modulação algorítmica introduz um novo tipo de governança, onde a decisão humana é gradativamente substituída por decisões automatizadas baseadas em dados. Essa dinâmica altera profundamente as relações sociais, criando um ambiente onde as opções e preferências dos indivíduos são constantemente geridas e ajustadas para maximizar o lucro das grandes plataformas, sem que os próprios indivíduos tenham consciência plena desse processo.¹¹²

A sociedade do controle é marcada pela opacidade e falta de transparência em relação aos processos de coleta e uso de dados. Os indivíduos, muitas vezes, desconhecem como suas informações são utilizadas para manipular suas experiências digitais. Essa falta de clareza contribui para uma forma de dominação mais sutil e eficaz, onde o controle é exercido não pela força, mas pela capacidade de moldar imperceptivelmente o comportamento e as decisões das pessoas.¹¹³

A introdução do conceito de vulnerabilidade algorítmica complementa a

¹⁰⁹ SOUZA, Joyce; AVELINO, Rodolfo; Silveira, Sérgio Amadeu da (Org.). *A sociedade de controle: manipulação e modulação nas redes digitais*. São Paulo: Hedra, 2018.

¹¹⁰ SILVEIRA, Sérgio Amadeu da; CASSINO, João Francisco; SOUZA, Joyce (orgs.). *Colonialismo de dados e modulação algorítmica: tecnopolítica, sujeição e guerra neoliberal*. São Paulo: Autonomia Literária, 2021.

¹¹¹ SILVEIRA, Sérgio Amadeu da; CASSINO, João Francisco; SOUZA, Joyce (orgs.). *Colonialismo de dados e modulação algorítmica: tecnopolítica, sujeição e guerra neoliberal*. São Paulo: Autonomia Literária, 2021.

¹¹² SILVEIRA, Sérgio Amadeu da; CASSINO, João Francisco; SOUZA, Joyce (orgs.). *Colonialismo de dados e modulação algorítmica: tecnopolítica, sujeição e guerra neoliberal*. São Paulo: Autonomia Literária, 2021.

¹¹³ SOUZA, Joyce; AVELINO, Rodolfo; Silveira, Sérgio Amadeu da (Org.). *A sociedade de controle: manipulação e modulação nas redes digitais*. São Paulo: Hedra, 2018.

discussão sobre a sociedade do controle, aprofundando a análise de como os sistemas digitais não apenas moldam comportamentos, mas também expõem os indivíduos a novos riscos. A vulnerabilidade algorítmica surge como uma consequência direta da modulação comportamental promovida pelas plataformas digitais, onde a opacidade e a complexidade dos algoritmos tornam os usuários ainda mais suscetíveis a manipulações e decisões automatizadas que escapam ao seu controle consciente.

A vulnerabilidade algorítmica diz respeito às desvantagens que os consumidores enfrentam devido à opacidade e complexidade dos algoritmos utilizados em plataformas digitais de comércio eletrônico. Esses algoritmos, muitas vezes desconhecidos pelos usuários, podem influenciar decisões de compra, segmentar informações e manipular preferências de forma quase imperceptível. A falta de transparência e a assimetria informacional tornam os consumidores suscetíveis a práticas abusivas, comprometendo sua liberdade de escolha e privacidade.⁷⁷

O direito à informação, conforme estabelecido no artigo 6, III, do Código de Defesa do Consumidor (Lei 8.078/1990), é um dos direitos básicos dos consumidores.¹¹⁴ Esse direito é crucial, pois visa garantir que o consumidor tenha liberdade de escolha, sendo informado sobre os riscos e benefícios do produto ou serviço para tomar uma decisão consciente. No entanto, a ordem econômica vigente, caracterizada pela predominância de grandes corporações e pela alta competitividade, muitas vezes resulta na minimização de informações relevantes para o consumidor, favorecendo a maximização de lucros em detrimento da transparência.¹¹⁵

A ausência de informações claras e objetivas para os consumidores na contratação de serviços digitais no comércio eletrônico resulta em um consentimento viciado na coleta e no tratamento de dados pessoais. Apesar da regulamentação trazida pela Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), observa-se uma fraca adesão das plataformas às exigências legais durante a navegação no

¹¹⁴ Art. 6º São direitos básicos do consumidor:

[...]

III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; (Redação dada pela Lei nº 12.741, de 2012).

¹¹⁵ VERBICARO, Dennis. *O impacto do capitalismo de plataforma no agravamento da vulnerabilidade algorítmica do consumidor e do trabalhador*. Revista de Direito do Trabalho, vol. 223, p. 277-305, 2022.

ambiente digital, principalmente devido à atuação insuficiente da Autoridade Nacional de Proteção de Dados no que tange ao princípio da finalidade (art. 6º, I, Lei 13.709/2018) e à necessidade de fornecer informações claras e adequadas para o consentimento inequívoco e informado (art. 5º, XII, Lei 13.709/2018). A ordem econômica influencia essa situação, pois a pressão para otimizar a monetização dos dados pessoais dos consumidores pode levar as empresas a negligenciarem a conformidade total com as regulamentações de proteção de dados.¹¹⁶

Outro ponto relacionado à informação é que os fornecedores devem informar aos consumidores sobre a utilização de inteligência artificial na tomada de decisões, pois o consumidor está sujeito ao que é oferecido no mercado, havendo um cerceamento de escolha.¹¹⁷ No contexto econômico, a concentração de poder nas mãos de grandes plataformas digitais limita a concorrência e restringe as opções dos consumidores, exacerbando a vulnerabilidade algorítmica.

Nesse contexto, é interessante a explicação de Baggio, que sustenta que o direito de informação do consumidor decorre da sua vulnerabilidade, uma vez que retrata a situação de submissão, de sujeição àquilo que é ofertado no mercado, ou seja, a sua situação de dependência em relação ao fornecedor e fragilidade na relação de consumo.¹¹⁸ O Código de Defesa do Consumidor tem por premissa proporcionar equilíbrio nas relações entre consumidor e fornecedor, daí porque a necessidade de transparência nesta relação. O fornecedor tem o dever legal de informar a parte em desvantagem a respeito dos dados fáticos, técnicos e científicos, que deverão estar presentes na oferta.

Entretanto, isso não acontece na utilização de inteligência artificial nas relações de consumo no comércio eletrônico, visto que os usuários muitas vezes não sabem se determinada plataforma usa ou não IA. Esse problema é exacerbado pela linguagem técnica e pelas informações abundantes e muitas vezes sem importância contidas nos termos de serviço. Assim, não basta apenas fornecer informações, é essencial destacar as mais relevantes no contexto da contratação. Assim, é preciso enfatizar os riscos e as principais características do negócio, como a utilização ou não

¹¹⁶ BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/2018/lei/l13709.htm. Acesso em: 07 jul. 2024.

¹¹⁷ VERBICARO, Dennis. *O impacto do capitalismo de plataforma no agravamento da vulnerabilidade algorítmica do consumidor e do trabalhador*. Revista de Direito do Trabalho, vol. 223, p. 277-305, 2022.

¹¹⁸ BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Editora Revista dos Tribunais, 2012.

de IA naquela plataforma.¹¹⁹ A falta de regulamentação adequada no uso de IA nas transações comerciais reflete uma lacuna na ordem econômica, que ainda não está totalmente adaptada para lidar com os desafios da economia digital.

Deve-se tornar obrigatório que a plataforma informe se utiliza IA na tomada de decisões e em quais contextos. O não cumprimento desse dever fundamental nas relações de consumo resulta em uma grande assimetria informacional entre usuários e fornecedores, uma vez que as plataformas sabem tudo sobre os consumidores, enquanto os dados dessas empresas permanecem inacessíveis para o consumidor. A ordem econômica, que privilegia a eficiência e a inovação tecnológica, muitas vezes negligencia a necessidade de proteger adequadamente os consumidores contra essas assimetrias.

Essa assimetria é agravada quando se nota que a vulnerabilidade informacional assume contornos sociais, pois as populações carentes têm menos acesso à informação e estão sob mais riscos. Verbicaro e Montão apontam a crescente preocupação não só com a proteção dos dados, mas também com a necessidade de garantir que os consumidores tenham informações acessíveis e claras para que possam tomar decisões bem informadas. No contexto da ordem econômica, a desigualdade de acesso à informação e aos recursos digitais reforça as disparidades socioeconômicas existentes.¹²⁰

Diante desse cenário, é imperativo que haja um esforço conjunto entre legisladores, órgãos reguladores e empresas para garantir que os direitos dos consumidores sejam protegidos de maneira eficaz no ambiente digital. A implementação de políticas de transparência e de práticas éticas no uso de algoritmos e inteligência artificial é essencial para mitigar a vulnerabilidade algorítmica. A ordem econômica deve evoluir para incorporar esses princípios, promovendo um ambiente de mercado mais equilibrado e justo, onde os consumidores possam exercer seus direitos plenamente e com segurança.

1.3.3 Vulnerabilidade na proteção de dados

Com a evolução do comércio eletrônico, a conveniência proporcionada aos

¹¹⁹ VERBICARO, Dennis; VIEIRA, Janaína. *A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço*. Revista de Direito do Consumidor, v. 134, p. 195-226, 2021.

¹²⁰ VERBICARO, Dennis; MONTÃO, Vanessa Maria Dias. *Empoderamento do consumidor no ambiente virtual*. Revista Jurídica (FURB), v. 26, p. e9910-e9910, 2022.

consumidores que podem fazer compras sem sair de casa resultou em um aumento massivo na propagação e no uso inconsciente de dados pessoais. Ao se cadastrar em um site para realizar uma compra, o consumidor fornece dados altamente pessoais sem ter ciência do que será feito com eles, um aspecto crucial na sociedade da informação. Bioni esclarece que os dados de consumo podem ser utilizados para moldar um perfil do indivíduo com base em seu histórico de compras. Através disso, é possível construir um perfil do consumidor para ajustar preços de acordo com sua capacidade econômica (discriminação de preços).¹²¹

Esse processo é conhecido como *profiling*, que segundo Bioni, envolve a criação de um perfil do indivíduo com base em seus dados pessoais, influenciando suas decisões. Tudo é calibrado com base nesses estereótipos; inclusive, o próprio conteúdo acessado na *internet*.¹²² A ordem econômica atual, que valoriza a maximização de lucros e a eficiência de mercado, incentiva práticas de *profiling* para segmentação de mercado e personalização de ofertas, potencializando a vulnerabilidade do consumidor.

Controlar esses dados e decidir quem os utilizará e para quais fins é um poder significativo na sociedade da informação. A proteção de dados introduz uma nova dimensão aos direitos da personalidade, visando o livre desenvolvimento da personalidade sem interferências. O acesso a dados pessoais vai além da simples escolha individual, afetando o direito fundamental à privacidade, e requerendo mecanismos de proteção desses dados.¹²³ No contexto econômico, a coleta e utilização de dados pessoais tornam-se um ativo valioso, influenciando as estratégias de mercado e a competitividade das empresas.

No Brasil, a proteção de dados pessoais foi reconhecida como um direito fundamental na Declaração de Santa Cruz de La Sierra, em 15 de novembro de 2003, durante a XIII Cumbre Ibero-Americana de Chefes de Estado e de Governo. Esse documento, que o Brasil assinou, estabelece em seu artigo 45 que a proteção de dados pessoais é um direito fundamental, enfatizando a importância de proteger a

¹²¹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020.

¹²² BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020.

¹²³ OLIVEIRA, Tassara Onofre de. *Gestão de dados pessoais: uma análise de casos concretos a partir do ordenamento jurídico brasileiro*. 109 f. Dissertação (Mestrado em Gestão nas organizações aprendentes) – Curso de Pós-Graduação em Gestão

privacidade dos cidadãos.¹²⁴ Essa declaração reflete um reconhecimento da necessidade de adaptação das normas econômicas e de mercado às novas realidades digitais.

Nesse sentido, os avanços tecnológicos revolucionaram a manipulação de dados. E devido a isso, há uma preocupação crescente quanto ao direito à privacidade, pois implica no controle que o indivíduo possui sobre suas próprias informações. A economia digital cria um ambiente em que os dados são constantemente coletados, analisados e comercializados, exacerbando os riscos de vulnerabilidade para os consumidores.

A Lei n. 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), estabelece normas para o uso, proteção e transferência de dados pessoais no Brasil. Esta legislação garante maior controle dos cidadãos sobre suas informações pessoais, exigindo consentimento explícito para a coleta e uso dos dados e fornecendo ao usuário opções para visualizar, corrigir e excluir essas informações.¹²⁵

É relevante destacar que esse marco regulatório foi desenvolvido a partir da revisão e atualização de legislações já existentes, com o objetivo de se adaptar à nova realidade social. No entanto, para focar no tema central, são citadas apenas as leis esparsas que contribuíram para a criação da LGPD e que estão relacionadas à proteção dos dados dos consumidores.

A vulnerabilidade na proteção de dados dos consumidores do comércio eletrônico é uma preocupação crescente na era digital. Com o aumento das transações *on-line*, os consumidores frequentemente compartilham informações pessoais e financeiras em plataformas de compras, o que os expõe a riscos significativos. Hackers e outras entidades mal-intencionadas podem explorar falhas de segurança nos sistemas das empresas para acessar e utilizar esses dados de maneira ilícita, resultando em fraudes, roubo de identidade e outras formas de abuso.¹²⁶ Esses riscos refletem um desequilíbrio na ordem econômica, onde a segurança e a confiança dos consumidores podem ser comprometidas pela busca de

¹²⁴ SARAIVA NETO, Pery; FENILI, Maiara Bonetti. *Novos marcos legais sobre proteção de dados pessoais e seus impactos na utilização e tratamento de dados para fins comerciais*. Revista de Estudos Jurídicos e Sociais - REJUS ON LINE [S.I.], v. 1, n. 1, dez. 2018.

¹²⁵ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/2018/lei/l13709.htm. Acesso em: 07 jul. 2024.

¹²⁶ VIEIRA, Samira Santos Souza; DANTAS, Wellson Rosário Santos. *Os desafios da proteção do consumidor no comércio eletrônico*. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 10, n. 5, p. 2721-2732, 2024.

eficiência e inovação por parte das empresas.

Apesar de a Lei de proteção de dados se basear em legislações anteriores, ela não mantém uma continuidade simples com as normas passadas. O que se observa, de fato, é uma nova abordagem jurídica e sistemática para a regulamentação do uso de informações pessoais e para garantir os direitos dos titulares dos dados, que não poderia, de forma alguma, ser implementada com base apenas nas leis anteriores.

Assim, a LGPD objetiva estabelecer regras claras para o tratamento de dados pessoais. A lei abrange conceitos fundamentais, princípios de proteção de dados, um rol de hipóteses que permitem o tratamento de dados pessoais, entre outros aspectos legais essenciais para a compreensão e aplicação do tema. Dessa forma, destaca-se a importância da Lei n. 13.709/2018 na proteção dos dados dos consumidores no comércio eletrônico, pois muitos aspectos tratados na lei são aplicáveis às relações de consumo no ambiente virtual. A legislação representa um esforço para equilibrar a ordem econômica com a necessidade de proteger os consumidores contra abusos e práticas injustas no ambiente digital.

2 DARK PATTERNS: ABUSO DA PRIVACIDADE E ASSÉDIO AO CONSUMIDOR NO COMÉRCIO ELETRÔNICO

Este capítulo examina o fenômeno dos *dark patterns* no comércio eletrônico, práticas de *design* enganosas que manipulam a experiência do usuário para influenciar decisões de consumo, muitas vezes em detrimento da privacidade e autonomia do consumidor. Assim, será explorada a definição e a origem desses padrões obscuros, destacando como a assimetria de *design* contribui para um ambiente de interação desequilibrado entre consumidores e plataformas digitais. A análise inclui ainda uma revisão da legislação estrangeira que visa regular o uso de *dark patterns*, bem como uma discussão sobre a fragilização dos direitos de privacidade e autonomia dos consumidores nesse contexto. Por fim, serão abordados os princípios e diretrizes éticas estabelecidos pelo Guia nº 3/2022 do Comitê Europeu para a Proteção de Dados (EDPB), que buscam orientar a prática responsável no uso de *designs* que respeitem os direitos fundamentais dos consumidores.

2.1 DARK PATTERNS

Antes de aprofundar no conceito de *dark patterns* e sua origem, é essencial compreender o papel fundamental que o *design* de interface desempenha na experiência do usuário em ambientes digitais. O *design* de interface não se limita à estética ou à funcionalidade; ele exerce uma influência significativa sobre as decisões dos consumidores, moldando a forma como interagem com as plataformas digitais. Ao explorar a interseção entre *design* e comportamento humano, torna-se evidente que as escolhas feitas no desenvolvimento de interfaces podem tanto empoderar os usuários quanto manipulá-los. Dessa forma, a discussão sobre *dark patterns* insere-se em um contexto mais amplo de responsabilidade ética no *design* de interfaces, onde a linha entre influência legítima e manipulação abusiva se torna tênue e, muitas vezes, imperceptível para o consumidor.

2.1.1 Conceito e origem

O conceito de *dark patterns* ganhou notoriedade na literatura após ser

introduzido por Brignull em 2010.¹²⁷ O supracitado autor definiu essas práticas como técnicas de *design* de interface criadas para influenciar de maneira sutil e inconsciente as escolhas dos usuários, levando-os a realizar ações que não pretendiam, como adquirir produtos ou se inscrever em serviços indesejados. Esses padrões se tratam de truques usados em *sites* e aplicativos que fazem você realizar ações que não planejava, como comprar ou se inscrever em algo. A manipulação intencional dessas interfaces digitais visa direcionar o comportamento dos usuários para escolhas que beneficiam as empresas, frequentemente em detrimento da vontade e dos interesses dos próprios consumidores.¹²⁸

A origem dos *dark patterns* está profundamente ligada ao avanço da economia comportamental, especialmente aos estudos de Tversky e Kahneman, que, em 1974, publicaram um artigo pioneiro sobre os vieses cognitivos que influenciam as decisões humanas.¹²⁹ Esses pesquisadores mostraram que as decisões das pessoas são frequentemente moldadas por heurísticas, que são atalhos mentais que podem levar a julgamentos enviesados.¹³⁰ Essas descobertas foram mais tarde apropriadas por empresas para criar interfaces digitais que exploram essas vulnerabilidades cognitivas, resultando em padrões de *design* que manipulam os usuários de maneira sutil, mas eficaz. Essas práticas se aproveitam de fraquezas cognitivas humanas, como a propensão a agir impulsivamente, a dificuldade em prestar atenção a detalhes e a complexidade na compreensão de certas informações.¹³¹

Com o avanço do comércio eletrônico, o espaço para a aplicação de *dark patterns* se expandiu, utilizando a maleabilidade das interfaces digitais para influenciar o comportamento dos usuários de forma mais precisa do que em mídias tradicionais,

¹²⁷ BRIGNULL, Harry. *Dark Patterns*. 2010. Disponível em: <https://darkpatterns.org>. Acesso em: 12 ago. 2024.

¹²⁸ ROLIM, Fernanda Silva Scheffer. *Publicidade enganosa e abusiva: a responsabilização e o fenômeno do dark patterns*. Monografia (Bacharelado em Direito) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023. p. 37.

¹²⁹ A economia comportamental é uma área de estudo relativamente nova, originada da integração, pela economia, de teorias e descobertas empíricas advindas da psicologia. Recentemente, esse campo tem se expandido com as contribuições das neurociências e de outras ciências sociais e humanas. Dessa forma, buscando uma compreensão mais realista das escolhas individuais e dos processos de mercado, os economistas comportamentais procuram incluir fatores emocionais, conscientes e inconscientes que influenciam o comportamento humano.

¹³⁰ TVERSKY, Amos; KAHNEMAN, Daniel. *Judgment under uncertainty: heuristics and biases*. Science, v. 185, ed. 4157, p. 1124-1131, 1974. Disponível em: <https://www.science.org/doi/10.1126/science.185.4157.1124>. Acesso em: 02 ago. 2024.

¹³¹ THALER, Richard H.; SUNSTEIN, Cass R. *Nudge: Como tomar melhores decisões sobre saúde, dinheiro e felicidade*. Rio de Janeiro: Objetiva, 2019. E-book.

como a televisão ou os jornais.¹³² Esse fenômeno levanta questões éticas e legais, já que tais práticas podem ser interpretadas como formas de publicidade enganosa ou abusiva, dependendo da maneira como a informação é apresentada e da intenção de confundir o consumidor.¹³³

Thaler e Sunstein aprofundam a discussão ao demonstrar como pequenas mudanças no ambiente de decisão podem influenciar as escolhas das pessoas. Eles propõem o uso de *nudges*¹³⁴ para ajudar os indivíduos a tomarem decisões melhores para si mesmos. No entanto, quando essas técnicas são usadas de maneira manipulativa e sem transparência, elas dão origem aos *dark patterns*, que desviam os usuários para comportamentos que beneficiam as empresas em detrimento dos interesses dos consumidores.¹³⁵ Isso ilustra como uma abordagem originalmente pensada para o bem-estar pode ser deturpada para fins comerciais questionáveis.

Estudos têm revelado a extensão e a eficácia dos *dark patterns* em ambientes digitais. Pesquisas conduzidas por Mathur *et al.* e Gray *et al.* identificaram a presença generalizada dessas técnicas em uma ampla variedade de *sites* comerciais.¹³⁶ Esses estudos demonstram que os *dark patterns* são usados para induzir os consumidores a gastar mais ou fornecer mais informações pessoais do que fariam sob condições normais, evidenciando o impacto significativo dessas práticas sobre o comportamento de consumo.¹³⁷

Além de influenciar o comportamento de consumo, os *dark patterns* também têm sérias implicações para a privacidade dos usuários. Bösch *et al.* exploraram como essas práticas manipulativas são utilizadas para extrair mais dados pessoais dos usuários do que seria necessário ou esperado. Isso não só expõe os indivíduos a riscos maiores de violação de privacidade, mas também levanta questões éticas sobre o uso dessas estratégias por empresas que buscam maximizar lucros à custa da

¹³² ROLIM, Fernanda Silva Scheffer. *Publicidade enganosa e abusiva: a responsabilização e o fenômeno do dark patterns*. Monografia (Bacharelado em Direito) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023. p. 22.

¹³³ SPERANZA, Henrique de Campos Gurgel. *Publicidade enganosa e abusiva*. Revista Síntese de Direito Civil e Processual Civil, Porto Alegre, n. 83, 2013.

¹³⁴ São instrumentos da economia comportamental, uma área que integra aspectos da psicologia e da economia para compreender o processo de tomada de decisão dos indivíduos.

¹³⁵ THALER, Richard H.; SUNSTEIN, Cass R. *Nudge: Como tomar melhores decisões sobre saúde, dinheiro e felicidade*. Rio de Janeiro: Objetiva, 2019.

¹³⁶ GRAY, Colin M. et al. *The dark (patterns) side of UX design*, In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018.

¹³⁷ MATHUR, Arunesh et al. *Dark patterns at scale: Findings from a crawl of 11K shopping websites*. Proceedings of the ACM on Human-Computer Interaction, 2019.

proteção dos dados dos consumidores.¹³⁸

Zuboff, aprofunda a compreensão dos *dark patterns* ao relacioná-los com o conceito de capitalismo de vigilância. A autora argumenta que essas práticas fazem parte de um sistema mais amplo, em que as empresas não apenas monitoram, mas também moldam o comportamento dos consumidores para maximizar o lucro. Nesse contexto, os *dark patterns* são ferramentas que ajudam a concretizar o objetivo do capitalismo de vigilância, ou seja, manipular as escolhas dos usuários de maneira que favoreça os interesses comerciais, frequentemente em detrimento da autonomia e da privacidade individual.¹³⁹

No cenário internacional, a OCDE publicou um relatório em 2022 que reúne evidências e análises sobre o uso de *dark patterns*, destacando os prejuízos que essas práticas podem causar aos consumidores. A OCDE sublinha a necessidade de regulamentação para combater essas práticas e proteger os direitos dos consumidores, especialmente em um ambiente digital cada vez mais complexo e dinâmico.¹⁴⁰

A aplicação prática dos *dark patterns* foi analisada por Luguri e Strahilevit, que demonstraram como essas práticas podem reduzir substancialmente a autonomia dos consumidores. Os pesquisadores mostraram que os *dark patterns* são eficazes em induzir comportamentos específicos que favorecem as empresas, ao mesmo tempo em que comprometem a capacidade dos consumidores de tomar decisões informadas e voluntárias. Exemplos dessas práticas incluem obstáculos para cancelar assinaturas, botões com rótulos enganosos e renovações automáticas de serviços sem o consentimento claro do consumidor.¹⁴¹

No Brasil, o debate sobre *dark patterns* é particularmente relevante no contexto da proteção do consumidor, especialmente no que diz respeito ao Código de Defesa do Consumidor. O uso dessas técnicas manipulativas pode ser considerado uma violação dos direitos dos consumidores, ao enganá-los ou forçá-los a tomar decisões

¹³⁸ BÖSCH, Christoph et al. *Tales from the dark side: Privacy dark strategies and privacy dark patterns*. In: *Proceedings on Privacy Enhancing Technologies*, 2016, n. 4, p. 237-254.

¹³⁹ ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Rio de Janeiro: Intrínseca, 2020. E-book.

¹⁴⁰ OCDE. *Dark Commercial Patterns*. *OECD Digital Economy Papers*, No. 336, OECD Publishing, Paris, 2022. Disponível em: <https://doi.org/10.1787/44f5e846-en>. Acesso em: 11 ago. 2024.

¹⁴¹ LUGURI, Jamie; STRAHILEVITZ, Lior Jacob. *Shining a light on dark patterns*. *Journal of Legal Analysis*, v. 13, n. 1, p. 43-109, 2021.

que não fariam se estivessem plenamente informados.¹⁴² Apesar de a legislação brasileira, como a Lei Geral de Proteção de Dados (LGPD) e o Código de Defesa do Consumidor (CDC), não mencionar explicitamente os *dark patterns*, elas contêm disposições que podem ser usadas para proteger os consumidores contra essas práticas, oferecendo uma proteção que, embora indireta, é significativa.¹⁴³

Essas práticas impactam de forma mais intensa consumidores com vulnerabilidade agravada, como idosos, pessoas com pouca familiaridade com o ambiente digital ou com dificuldades de linguagem, destacando a importância de regulamentações que protejam esses grupos contra práticas abusivas e enganosas.¹⁴⁴ A conscientização sobre *dark patterns* tem aumentado, impulsionada por iniciativas como a *dark patterns Tip Line*, criada pelo *Digital Civil Society Lab* de Stanford, que permite que usuários relatem casos de manipulação *on-line*. Tais iniciativas têm o objetivo de educar o público e identificar práticas prejudiciais, especialmente aquelas que afetam comunidades vulneráveis.¹⁴⁵

Mesmo grandes empresas e plataformas de consumo são frequentemente criticadas por usar *dark patterns* de forma habitual, dificultando, por exemplo, o cancelamento de assinaturas ou criando uma falsa sensação de escassez de produtos. Embora comuns, essas práticas minam a confiança dos consumidores e podem gerar consequências negativas para as empresas a longo prazo. Finalmente, o crescente interesse de acadêmicos e reguladores internacionais por *dark patterns* ressalta a necessidade de um debate mais profundo sobre o tema no Brasil. Como conclui Jandrey, é essencial aumentar a conscientização sobre essas práticas manipulativas e desenvolver estratégias para garantir que os consumidores brasileiros sejam protegidos em um ambiente digital cada vez mais complexo e potencialmente prejudicial.¹⁴⁶ O avanço desse debate pode resultar em uma melhor proteção dos

¹⁴² MARQUES, Cláudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. *Dark patterns e padrões comerciais escusos*. Revista de Direito do Consumidor, São Paulo, v. 145, n. 32, p. 295-316, jan./fev. 2023.

¹⁴³ SAMPAIO, Marília de A. S.; JANDREY, Claudio L. *Dark Patterns e seu Uso no Mercado de Consumo*. Revista de Direito do Consumidor, v. 143, p. 231-257, set.-out. 2022.

¹⁴⁴ ROLIM, Fernanda Silva Scheffer. *Publicidade enganosa e abusiva: a responsabilização e o fenômeno do dark patterns*. Monografia (Bacharelado em Direito) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023.

¹⁴⁵ MARQUES, Cláudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. *Dark patterns e padrões comerciais escusos*. Revista de Direito do Consumidor, São Paulo, v. 145, n. 32, p. 295-316, jan./fev. 2023.

¹⁴⁶ JANDREY, Claudio L. *Dark Patterns e seu Uso no Mercado de Consumo*. Revista de Direito do Consumidor, v. 143, p. 231-257, set.-out. 2022.

direitos dos consumidores e maior transparência nas práticas de *design* de interfaces digitais.

Dada a crescente sofisticação e disseminação dessas práticas, a necessidade de regulamentações mais rigorosas se torna evidente. É fundamental proteger os consumidores dessas técnicas enganosas para assegurar que suas decisões sejam tomadas de forma informada e consciente.¹⁴⁷ Os *dark patterns* representam um desafio crescente para a ética e a legislação no *design* de interfaces digitais. Embora algumas dessas práticas sejam sutis, seus impactos podem ser significativos, especialmente para os consumidores mais vulneráveis. Por isso, regulamentação e conscientização são fundamentais para combater essas práticas e garantir a proteção dos direitos dos consumidores.¹⁴⁸

Assim, a compreensão dos *dark patterns* exige uma análise crítica não apenas de suas técnicas específicas, mas também de suas implicações mais amplas para a autonomia do consumidor e a ética no *design* digital. Ao explorar a origem e o impacto dessas práticas, fica claro que elas representam um desafio significativo para a proteção dos direitos dos consumidores em um mundo cada vez mais digitalizado. Diante disso, torna-se essencial aprofundar na análise dos aspectos gerais dessas práticas, explorando como elas se manifestam e de que forma podem ser combatidas por meio de regulamentações eficazes e conscientização do público.

2.1.2 Aspectos gerais: assimetria de *design*

A utilização dos *dark patterns* em plataformas digitais pode ser comparada às estratégias de manipulação econômica descritas por Akerlof e Shiller, a economia digital, ao explorar fraquezas cognitivas dos consumidores, cria um equilíbrio de mercado no qual a manipulação se torna uma ferramenta competitiva inevitável. Assim como a oferta das máquinas caça-níqueis, que exploram impulsos e compulsões humanas para garantir lucro, as plataformas digitais desenham suas interfaces de forma a capturar a atenção e influenciar decisões contrárias ao interesse dos

¹⁴⁷ SPERANZA, Henrique de Campos Gurgel. *Publicidade enganosa e abusiva*. Revista Síntese de Direito Civil e Processual Civil, Porto Alegre, n. 83, p. 43-45, 2020.

¹⁴⁸ DIAS, Lucia Ancona Lopez de Magalhães. *Publicidade e direito*. 2. ed. São Paulo: Revista dos Tribunais, 2013.

consumidores, resultando em escolhas não racionais.¹⁴⁹

De forma semelhante ao que Akerlof e Shiller explicam sobre os mecanismos de "macacos no ombro", o comportamento dos consumidores em ambientes digitais é frequentemente guiado por padrões que exploram suas vulnerabilidades emocionais e cognitivas. Essas plataformas identificam momentos de fraqueza para tirar proveito, manipulando a jornada de compra para criar uma falsa sensação de necessidade ou urgência. Isso reflete uma lógica de mercado que prioriza lucros imediatos, em detrimento da proteção dos consumidores e do equilíbrio econômico saudável.¹⁵⁰

Além disso, a crítica dos autores à ideia do equilíbrio de mercado destaca que, em ambientes não regulados, a manipulação se perpetua como um padrão econômico competitivo. No contexto dos *dark patterns*, a ausência de uma regulação eficaz permite que as plataformas atuem livremente, maximizando lucros às custas dos direitos fundamentais dos consumidores.¹⁵¹ Diferente da persuasão legítima, que busca convencer o consumidor de forma clara e honesta, a manipulação através dos *dark patterns* visa limitar a liberdade de escolha, ocultando suas verdadeiras intenções e levando o consumidor a tomar decisões sem perceber que está sendo influenciado.

Como afirma Breton, a manipulação se caracteriza pela redução mais completa possível da liberdade de o público discutir ou de resistir ao que lhe é proposto. Essa estratégia deve ser invisível, já que seu desvelamento indicaria a existência de uma tentativa de manipulação.¹⁵² Empresas de *e-commerce* que utilizam *dark patterns* exploram as vulnerabilidades dos consumidores, criando interfaces que aparentam ser amigáveis, mas que na realidade induzem a comportamentos prejudiciais, como a realização de compras impulsivas ou desnecessárias.

A criação dessas interfaces não é acidental; elas são desenvolvidas com base em um profundo conhecimento da psicologia humana, permitindo que as empresas explorem as fraquezas cognitivas dos usuários. Mathur *et al.* destacam que os *dark patterns* podem levar a problemas financeiros, perdas patrimoniais, exposição de

¹⁴⁹ AKERLOF, George A.; SHILLER, Robert J. *Pescando tolos: a economia da manipulação e fraude*. Rio de Janeiro: Alta Books, 2016. p. 7-8.

¹⁵⁰ AKERLOF, George A.; SHILLER, Robert J. *Pescando tolos: a economia da manipulação e fraude*. Rio de Janeiro: Alta Books, 2016. p. 5-6.

¹⁵¹ AKERLOF, George A.; SHILLER, Robert J. *Pescando tolos: a economia da manipulação e fraude*. Rio de Janeiro: Alta Books, 2016. p. 7.

¹⁵² BRETON, Philippe. *A manipulação da palavra*. São Paulo: Loyola, 1999.

dados pessoais e até comportamentos compulsivos e viciantes.¹⁵³ Um exemplo típico de manipulação é o uso de técnicas que criam uma falsa sensação de urgência, levando o consumidor a acreditar que deve agir rapidamente para não perder uma oferta, quando, na verdade, a promoção ou a quantidade limitada de produtos é fictícia.

Essas interfaces são cuidadosamente projetadas para forçar ou enganar os consumidores, levando-os a tomar decisões que normalmente não tomariam se estivessem completamente informados.¹⁵⁴ A manipulação é particularmente eficaz em ambientes digitais, onde a clareza e a transparência são frequentemente comprometidas, deixando os consumidores ainda mais expostos a práticas comerciais enganosas. Essas táticas tiram proveito da falta de regulamentação específica e da complexidade das interfaces digitais para manipular o comportamento do consumidor de maneira furtiva e eficaz. Bösch *et al.* observam que a ideia de *dark patterns* foi amplamente aceita na engenharia de *software* e se espalhou para diversas áreas, incluindo a segurança de TI e a privacidade.¹⁵⁵

Um dos aspectos dos *dark patterns* é a assimetria no *design* das interfaces, que envolve a criação de botões ou opções de forma desigual, como destacar excessivamente a opção que a plataforma deseja que o consumidor escolha, minimizando as alternativas. Esse método guia o consumidor para uma decisão pré-estabelecida pela plataforma, muitas vezes contrária aos seus interesses. A prática de realçar uma opção específica, enquanto outras alternativas são apresentadas de forma menos visível ou acessível, induz o consumidor a fazer escolhas que não refletem necessariamente suas reais preferências ou necessidades. Essa assimetria no *design* visa manipular a tomada de decisão, direcionando o consumidor para o caminho que favorece os interesses da empresa, muitas vezes em detrimento da sua própria vontade.

Outra tática comum dos *dark patterns* é ocultar as escolhas do consumidor e

¹⁵³ MATHUR, Arunesh; ACAR, Gunes; FRIEDMAN, Michael J.; Lucherini, Elena; MAYER, Jonathan; CHETTY, Marshini; NARAYANAN, Arvind. *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*. Proceedings of the ACM on Human-Computer Interaction, v. 3, Issue CSCW, nov. 2019, Article nº 81, p. 1-32. Disponível em: <https://doi.org/10.1145/3359183>. Acesso em: 08 ago. 2024.

¹⁵⁴ SAMPAIO, Marília de Ávila e Silva; JANDREY, Cláudio Luiz. *Dark Patterns e seu uso no mercado de consumo*. Revista de Direito do Consumidor, v. 143, p. 231-257, 2022.

¹⁵⁵ BÖSCH, Christoph; ERB, Benjamin; KARGL, Frank; KOPP, Henning; PFATTHEICHER, Stefan. *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*. Proceedings on Privacy Enhancing Technologies, Issue 4 (October 2016), p. 237-254. Disponível em: <https://www.sciendo.com/article/10.1515/popets-2016-0038>. Acesso em: 10 ago. 2024.

as consequências dessas escolhas. Isso inclui dificultar a visualização de informações essenciais ou esconder detalhes importantes, induzindo o consumidor a tomar decisões com base em informações incompletas ou enganosas. A ocultação pode ocorrer de diversas maneiras, como esconder os custos reais de um serviço até a última etapa da compra ou ocultar informações sobre assinaturas automáticas em letras pequenas ou locais de difícil acesso. Essa prática é especialmente prejudicial porque mina a confiança do consumidor, que pode sentir-se enganado ao descobrir que fez uma escolha sem estar plenamente ciente de todas as implicações envolvidas.¹⁵⁶

A obstrução é outra característica central dos *dark patterns*, onde se dificulta o acesso do consumidor a informações ou ações que seriam benéficas para ele, como cancelar uma assinatura ou encontrar detalhes sobre a política de privacidade. Ao impor barreiras adicionais, como processos de cancelamento longos ou a necessidade de contato telefônico para resolver questões simples, as empresas criam um ambiente em que o consumidor é pressionado a manter serviços ou produtos que não deseja mais. Essa técnica de obstrução não só aumenta os lucros a curto prazo, mas também prejudica a experiência do consumidor, que se sente preso e manipulado.¹⁵⁷

Além disso, o uso de declarações omissas ou enganosas é outra tática frequente nos *dark patterns*. Isso pode incluir, por exemplo, ofertas limitadas que, na verdade, estão disponíveis para todos, ou informações propositalmente apresentadas de maneira confusa para induzir o consumidor ao erro.¹⁵⁸ A manipulação por meio de informações enganosas explora a tendência natural dos consumidores de confiar no que é apresentado pelas plataformas, assumindo que as informações são verdadeiras e completas. Quando as declarações são deliberadamente confusas ou enganosas, o consumidor é levado a fazer escolhas que beneficiam a plataforma, frequentemente em detrimento de seus próprios interesses ou segurança.

¹⁵⁶ BÖSCH, Christoph; ERB, Benjamin; KARGL, Frank; KOPP, Henning; PFATTHEICHER, Stefan. *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*. Proceedings on Privacy Enhancing Technologies, Issue 4 (October 2016), p. 237-254. Disponível em: <https://www.sciendo.com/article/10.1515/popets-2016-0038>. Acesso em: 10 ago. 2024.

¹⁵⁷ BRIGNULL, Harry. *Dark patterns: Deception vs. honesty in UI design*. A List Apart, Issue nº 338, 01 nov. 2011. Disponível em: <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/>. Acesso em: 07 ago. 2024.

¹⁵⁸ LUGURI, Jamie; STRAHILEVITZ, Lior Jacob. *Shining a Light on Dark Patterns*. Journal of Legal Analysis, v. 13, p. 55, 2021. Disponível em: <https://academic.oup.com/jla/article/13/1/43/5876811>. Acesso em: 06 ago. 2024.

Alguns *dark patterns* utilizam o que se chama de *emotional steering*, manipulando as emoções do consumidor para influenciar suas decisões. Isso pode ser feito ao apresentar informações de forma a provocar medo, urgência ou insegurança, levando o consumidor a agir de maneira impulsiva e menos racional. A exploração das emoções humanas é uma ferramenta poderosa nas mãos dos desenvolvedores de *dark patterns*, que podem, por exemplo, criar um falso senso de urgência para persuadir o consumidor a comprar algo imediatamente. Esse tipo de manipulação emocional é particularmente eficaz porque atinge o consumidor em um nível psicológico profundo, comprometendo sua capacidade de tomar decisões conscientes.¹⁵⁹

Um *dark pattern* frequentemente observado é a *forced action* (ação forçada), onde o consumidor é obrigado a realizar uma ação indesejada para poder prosseguir com uma tarefa desejada, como fornecer informações pessoais para acessar um serviço ou produto gratuito. Essa prática elimina a verdadeira autonomia do consumidor sobre suas decisões.¹⁶⁰ Forçar o consumidor a realizar uma ação específica, sob pena de não conseguir acessar o que deseja, cria uma dinâmica em que a liberdade de escolha é severamente limitada. Essa tática é particularmente problemática porque muitas vezes implica a coleta de dados pessoais que o consumidor não gostaria de compartilhar, mas sente-se compelido a fazê-lo para alcançar seu objetivo.¹⁶¹

Muitos *dark patterns* são projetados para dificultar o acesso a informações claras e transparentes, como esconder termos e condições importantes em textos longos e difíceis de entender ou dificultar o acesso a configurações de privacidade. Essa falta de transparência prejudica a capacidade do consumidor de tomar decisões informadas e conscientes.¹⁶² A transparência é um princípio fundamental nas relações

¹⁵⁹ BÖSCH, Christoph; ERB, Benjamin; KARGL, Frank; KOPP, Henning; PFATTHEICHER, Stefan. *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*. Proceedings on Privacy Enhancing Technologies, Issue 4 (October 2016), p. 237-254. Disponível em: <https://www.sciendo.com/article/10.1515/popets-2016-0038>. Acesso em: 10 ago. 2024.

¹⁶⁰ MATHUR, Arunesh; ACAR, Gunes; FRIEDMAN, Michael J.; Lucherini, Elena; MAYER, Jonathan; CHETTY, Marshini; NARAYANAN, Arvind. *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*. Proceedings of the ACM on Human-Computer Interaction, v. 3, Issue CSCW, nov. 2019, Article nº 81, p. 1-32. Disponível em: <https://doi.org/10.1145/3359183>. Acesso em: 08 ago. 2024.

¹⁶¹ BRIGNULL, Harry. *Dark patterns: Deception vs. honesty in UI design*. A List Apart, Issue nº 338, 01 nov. 2011. Disponível em: <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/>. Acesso em: 07 ago. 2024.

¹⁶² BÖSCH, Christoph; ERB, Benjamin; KARGL, Frank; KOPP, Henning; PFATTHEICHER, Stefan. *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*. Proceedings on Privacy

de consumo, e a sua ausência, provocada intencionalmente pelos *dark patterns*, gera um ambiente onde o consumidor não consegue exercer plenamente seus direitos. Quando informações são escondidas ou apresentadas de maneira a desencorajar a leitura ou compreensão, o consumidor fica em desvantagem, sendo levado a concordar com termos ou adquirir produtos e serviços sem entender completamente as consequências.

As plataformas que utilizam *dark patterns* frequentemente observam um crescimento em adesões e lucros a curto prazo, pois conseguem manipular os consumidores a realizar compras ou assinaturas que normalmente não fariam. No entanto, essa estratégia tende a levar a uma estagnação ou abandono da plataforma quando os consumidores percebem que foram enganados, comprometendo a fidelidade do cliente a longo prazo.¹⁶³ Embora essas táticas possam ser lucrativas inicialmente, elas comprometem a reputação da empresa e a confiança do consumidor, o que, em última análise, pode resultar em perda de clientes e danos à marca. A percepção de que uma empresa está utilizando práticas enganosas pode desencadear reações negativas, tanto no nível individual quanto coletivo, levando a uma perda significativa de credibilidade e de mercado.

Essas práticas de manipulação, como discutido por Mathur *et al.*, demonstram como os *dark patterns* podem explorar vulnerabilidades e influenciar decisões de consumo e também destacam os riscos éticos e legais associados ao seu uso. A longo prazo, a utilização de *dark patterns* não só prejudica o consumidor, mas também cria um ambiente de desconfiança e aumenta a necessidade de regulamentação mais rígida para proteger os direitos dos consumidores. No Brasil, apesar da existência de legislações como o Código de Defesa do Consumidor e o Marco Civil da Internet, ainda há lacunas na regulação específica das práticas digitais, especialmente no que se refere aos *dark patterns*. A ausência de sanções mais rigorosas e específicas para essas práticas abusivas permite que elas continuem a ser amplamente utilizadas pelas empresas, comprometendo a integridade e a autonomia dos consumidores.

Em resumo, a manipulação por meio de *dark patterns* no *e-commerce* representa uma séria ameaça à autonomia e à liberdade de escolha dos

Enhancing Technologies, Issue 4 (October 2016), p. 237-254. Disponível em: <https://www.sciendo.com/article/10.1515/popets-2016-0038>. Acesso em: 10 ago. 2024.

¹⁶³ SAMPAIO, Marília de Ávila e Silva; JANDREY, Cláudio Luiz. *Dark Patterns e seu uso no mercado de consumo*. Revista de Direito do Consumidor, v. 143, p. 231-257, 2022.

consumidores. A resposta a esse desafio deve incluir tanto uma regulamentação mais rigorosa dessas práticas quanto a promoção de uma educação digital que empodere os consumidores, permitindo-lhes exercer plenamente seus direitos no ambiente digital. A conscientização sobre essas práticas e a pressão por transparência são passos essenciais para mitigar os efeitos negativos dos *dark patterns* e promover um ambiente digital mais justo e ético.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) sugere a necessidade de instrumentos legislativos mais amplos para proteger os consumidores no ambiente digital. A utilização de *dark patterns* não só prejudica o consumidor, mas também compromete sua confiança na empresa, exigindo um esforço conjunto para garantir que os direitos dos consumidores sejam plenamente respeitados e que práticas manipuladoras sejam combatidas de forma eficaz.¹⁶⁴

À medida que cresce a conscientização sobre os impactos negativos dos *dark patterns* no comércio eletrônico, muitos países têm buscado soluções legais para mitigar essas práticas abusivas e proteger os consumidores de forma mais eficaz. Analisar a legislação de direito estrangeiro sobre o uso de *dark patterns* permite identificar abordagens inovadoras e eficazes já adotadas por outras nações, servindo de referência para o aprimoramento das normativas brasileiras e a promoção de um ambiente digital mais justo e transparente.

2.2 LEGISLAÇÃO DO DIREITO ESTRANGEIRO SOBRE A UTILIZAÇÃO DE *DARK PATTERNS*

O estudo das legislações estrangeiras sobre a utilização de *dark patterns* revela um esforço global para proteger os consumidores contra práticas comerciais enganosas que comprometem sua autonomia e capacidade de decisão. Em diversas jurisdições, como a União Europeia e os Estados Unidos, regulamentos rigorosos têm sido implementados para combater essas táticas manipulativas, que exploram vulnerabilidades cognitivas e comportamentais dos usuários. Este tópico analisará de maneira detalhada as principais iniciativas legais adotadas em diferentes países,

¹⁶⁴ ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Implementation toolkit on legislative actions for consumer protection enforcement co-operation*. OECD Digital Economy Papers, n. 310, 17 jun. 2021, 70 p. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/implementation-toolkit-on-legislative-actions-for-consumer-protection-enforcement-co-operation_eddc57-en. Acesso em: 14 ago. 2024.

destacando os avanços e desafios enfrentados na construção de um ambiente digital mais transparente e ético.

A União Europeia tem se destacado na regulamentação contra os *dark patterns*, especialmente através da Diretiva 2005/29/CE, que foca em práticas comerciais desleais. Essa diretiva visa proteger os consumidores contra práticas que exploram suas vulnerabilidades cognitivas e comportamentais, assegurando que as empresas não possam influenciar as escolhas dos consumidores de forma enganosa. Além disso, o Regulamento Geral sobre a Proteção de Dados (GDPR) complementa essas proteções, exigindo transparência nas interfaces de usuário e garantindo que as informações sejam apresentadas de maneira clara e acessível. Lupiañez-Villanueva *et al.* destacam que essa abordagem integrada na UE tem sido essencial para enfrentar os desafios das novas tecnologias digitais.¹⁶⁵

A GDPR da União Europeia também aborda diretamente as questões de manipulação digital, estabelecendo normas rigorosas para a transparência e proteção dos dados dos consumidores. Além de proibir práticas que comprometem a autonomia dos usuários, a GDPR impõe multas significativas às empresas que violam essas normas, incentivando uma maior conformidade entre as grandes corporações digitais. Yeung argumenta que a GDPR não só protege os dados pessoais dos consumidores, mas também garante que as escolhas feitas em plataformas digitais sejam informadas e voluntárias, fortalecendo a confiança no ambiente digital europeu.¹⁶⁶

Um estudo conduzido pela Comissão Europeia sobre práticas comerciais desleais no ambiente digital, detalhado por Lupiañez-Villanueva *et al.*, revelou a extensão alarmante do uso de *dark patterns* em sites e aplicativos populares. A descoberta de que 97% dos sites analisados utilizam pelo menos uma forma de *dark pattern* sublinha a necessidade urgente de uma regulamentação mais rigorosa e de uma maior conscientização dos consumidores. Além disso, o estudo sugere que a combinação de diferentes tipos de *dark patterns* pode aumentar a eficácia dessas práticas manipulativas, tornando ainda mais difícil para os consumidores identificarem

¹⁶⁵ LUPIÁÑEZ-VILLANUEVA, F.; BOLUDA, A.; BOGLIACINO, F. et al. *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation – final report*, 2022. Comissão Europeia. Direção-Geral da Justiça e dos Consumidores. Disponível em: <https://data.europa.eu/doi/10.2838/859030>. Acesso em: 07 ago. 2024.

¹⁶⁶ YEUNG, Karen. *'Hypertext': big data as a mode of regulation by design*, 02.05.2016. Information, Communication & Society (2016) 1,19, TLI Think! Paper 28/2016. Disponível em: <https://ssrn.com/abstract=2807574>. Acesso em: 07 ago. 2024.

e evitem essas armadilhas.¹⁶⁷

Na União Europeia, o Regulamento (EU) 2022/2065 sobre serviços digitais marcou um avanço significativo na proteção dos consumidores contra práticas desleais em plataformas *on-line*. Esse regulamento proibiu explicitamente o uso de *dark patterns* em interfaces digitais, reconhecendo que essas práticas distorcem ou prejudicam a capacidade dos usuários de fazer escolhas informadas. A legislação europeia vai além de condenar essas práticas, estabelecendo diretrizes claras para que as empresas evitem qualquer forma de manipulação que possa influenciar negativamente o comportamento dos consumidores. Adotando uma abordagem abrangente, o regulamento europeu busca garantir que os direitos dos consumidores sejam respeitados em todas as interações com plataformas digitais, promovendo um ambiente mais transparente e ético.¹⁶⁸

Além das ações nacionais, a União Europeia, por meio do *European Data Protection Board (EDPB)*, que será mais detalhado em tópico específico, publicou diretrizes específicas para combater os *dark patterns* em redes sociais. Essas diretrizes incluem recomendações detalhadas sobre como identificar e evitar práticas enganosas que possam manipular os usuários. O guia enfatiza a necessidade de transparência e clareza na comunicação com os consumidores, alertando contra técnicas que possam distorcer a percepção ou escolhas dos usuários. Essa abordagem preventiva busca não apenas punir as violações, mas também educar empresas e consumidores sobre as melhores práticas para interações digitais seguras e transparentes.¹⁶⁹

Nos Estados Unidos, por sua vez, a *Federal Trade Commission (FTC)* tem desempenhado um papel fundamental na luta contra práticas comerciais enganosas, incluindo o uso de *dark patterns*. Embora o termo não seja explicitamente mencionado em muitas decisões judiciais, a FTC tem combatido práticas que claramente se

¹⁶⁷ LUPIÁÑEZ-VILLANUEVA, F.; BOLUDA, A.; BOGLIACINO, F. et al. *Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation – final report*, 2022. Comissão Europeia. Direção-Geral da Justiça e dos Consumidores. Disponível em: <https://data.europa.eu/doi/10.2838/859030>. Acesso em: 07 ago. 2024.

¹⁶⁸ UNIÃO EUROPEIA. *Regulamento (EU) 2022/2065, de 19.10.2022*. Artigo 67. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065&from=EN>. Acesso em: 09 ago. 2024.

¹⁶⁹ UNIÃO EUROPEIA. *European Data Protection Board*. Guidelines 3/2022 on dark patterns in social media interfaces: how to recognise and avoid them. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 10 ago. 2024.

enquadram nessa categoria, como a dificuldade em cancelar serviços e a apresentação enganosa de informações. Luguri e Strahilevitz enfatizam que a eficácia dessas ações regulatórias depende da capacidade da FTC de continuamente atualizar suas diretrizes e adaptar suas estratégias para acompanhar as inovações tecnológicas do mercado digital.¹⁷⁰

Nos Estados Unidos, os Estados do Colorado e da Califórnia lideraram ao criar regulamentações que reconhecem a complexidade dos chamados *dark patterns* na coleta de dados pessoais. Essas leis consideram que o consentimento não é válido se for obtido por meio de técnicas que manipulam ou confundem os usuários, comprometendo sua autonomia. O objetivo dessas normas é proteger os consumidores de práticas que os levem a tomar decisões desfavoráveis sem plena consciência. Tanto a *California Consumer Privacy Act (CCPA)* quanto as legislações similares no Colorado consideram as interfaces de usuário projetadas para influenciar ou coagir consumidores, de forma dissimulada, como graves violações dos direitos dos consumidores. Essa postura coloca essas regiões na vanguarda do combate aos padrões obscuros, servindo de exemplo para outras jurisdições que ainda não regulamentaram o tema.¹⁷¹

Em nível federal nos EUA, embora ainda não exista uma legislação abrangente que trate de todos os tipos de padrões obscuros, a FTC tem focado em casos onde práticas comerciais claramente prejudicam os consumidores, como no caso da empresa Vonage, multada por dificultar o cancelamento de serviços, obrigando os consumidores a manterem assinaturas indesejadas. A ação contra a Vonage ressalta a importância de as empresas facilitarem tanto a contratação quanto o cancelamento de serviços, garantindo que os consumidores possam exercer plenamente seus direitos de escolha. Esse tipo de ação regulatória demonstra o compromisso da FTC em proteger os consumidores contra práticas enganosas que exploram a falta de familiaridade ou vulnerabilidade dos usuários em ambientes digitais.¹⁷²

Outro exemplo significativo da atuação da FTC foi a ação contra a *Epic Games*,

¹⁷⁰ LUGURI, Jamie; STRAHILEVITZ, Lior Jacob. *Shining a light on dark patterns*. Journal of Legal Analysis, v. 13, n. 1, p. 43-109, 2021. Disponível em: <https://doi.org/10.1093/jla/laaa006>. Acesso em: 05 ago. 2024.

¹⁷¹ LUGURI, Jamie; STRAHILEVITZ, Lior Jacob. *Shining a light on dark patterns*. Journal of Legal Analysis, v. 13, n. 1, p. 43-109, 2021. Disponível em: <https://doi.org/10.1093/jla/laaa006>. Acesso em: 05 ago. 2024.

¹⁷² MATHUR, Arunesh et al. *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*. Proceedings of the ACM Human-Computer Interaction, [s.l.], v. 3, article 81, p. 1-32, nov. 2019. Disponível em: <https://dl.acm.org/doi/10.1145/3359183>. Acesso em: 07 ago. 2024.

desenvolvedora do jogo *Fortnite*. A empresa foi multada por diversas infrações, incluindo o uso de padrões obscuros que facilitavam compras inadvertidas *on-line*, especialmente por crianças. A empresa também foi acusada de alterar opções de privacidade dos usuários sem o devido consentimento, o que foi fortemente criticado pela FTC.¹⁷³ O caso da *Epic Games* exemplifica como os *dark patterns* podem ser usados para explorar consumidores com vulnerabilidade agravada, manipulando-os a realizar ações que não tomariam se estivessem plenamente informados. A multa e as medidas corretivas impostas pela FTC destacam a seriedade com que essas práticas são tratadas e a necessidade de constante vigilância para proteger os direitos dos consumidores no ambiente digital.

Por sua vez, a França tem sido um dos países mais ativos na aplicação dessas normas europeias, especialmente através da *Commission Nationale de l'Informatique et des Libertés (CNIL)*. Em janeiro de 2022, a CNIL multou *Google* e *Facebook* por práticas relacionadas ao uso de *cookies*. Ambas as empresas facilitaram a aceitação de *cookies* com um único clique, enquanto dificultavam a rejeição, criando uma clara assimetria nas escolhas dos usuários.¹⁷⁴ Essas práticas foram caracterizadas como *dark patterns* de obstrução e manipulação de interfaces, uma vez que favoreciam os interesses comerciais das empresas em detrimento da privacidade e autonomia dos consumidores. A ação da CNIL exemplifica a importância da aplicação rigorosa das leis para coibir práticas que minam os direitos dos consumidores e subvertem a confiança nas interações digitais.¹⁷⁵

Na Alemanha, a atuação da *Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)* têm desempenhado papel importante na proteção dos consumidores, especialmente no setor financeiro. Em novembro de 2022, a BaFin proibiu o uso de *dark patterns* em plataformas de negociação operadas por instituições financeiras e serviços de crédito. A agência alemã argumentou que essas práticas não apenas violam os direitos dos consumidores, mas também comprometem a integridade do

¹⁷³ UNITED STATES OF AMERICA. *Federal Trade Commission*. Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges. Disponível em: <https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations>. Acesso em: 09 ago. 2024.

¹⁷⁴ FRANCE. *Commission Nationale de l'Informatique et des Libertés*. Cookies: la CNIL sanctionne GOOGLE à hauteur de 150 millions d'euros et FACEBOOK à hauteur de 60 millions d'euros pour non-respect de la loi. Disponível em: <https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros-et-facebook-hauteur-de-60-millions>. Acesso em: 06 ago. 2024.

¹⁷⁵ LUGURI, Jamie; STRAHILEVITZ, Lior Jacob. *Shining a light on dark patterns*. *Journal of Legal Analysis*, v. 13, n. 1, p. 43-109, 2021. Disponível em: <https://doi.org/10.1093/jla/laaa006>. Acesso em: 05 ago. 2024.

sistema financeiro, induzindo os usuários a tomar decisões contrárias aos seus interesses. A atuação da BaFin exemplifica como a aplicação de normas contra padrões obscuros pode ir além do comércio eletrônico, abrangendo setores críticos como o financeiro, onde a transparência e a confiança são fundamentais para o bom funcionamento do mercado.¹⁷⁶

No Reino Unido, a *Competition and Markets Authority (CMA)* tem sido proativa na investigação e ação contra o uso de *dark patterns* em plataformas digitais. Vale destacar a relevância da fiscalização rigorosa e da aplicação das leis existentes para garantir que as práticas comerciais digitais sejam justas e transparentes. A CMA tem conduzido estudos e emitido orientações que ajudam a identificar práticas manipulativas, especialmente em setores como *e-commerce* e serviços de assinatura, onde os *dark patterns* são mais comuns.¹⁷⁷

A Itália, por sua vez, tem adotado uma postura igualmente rigorosa contra os *dark patterns*. Em 2023, a *Garante per la Protezione dei Dati Personali* sancionou uma empresa por enganar usuários com opções de interface que os induziam a consentir com o uso de dados pessoais para fins de *marketing* sem o devido esclarecimento. Essa prática foi identificada como um padrão obscuro de dissimulação, onde informações essenciais foram ocultadas ou apresentadas de maneira confusa. A ação da *Garante* ilustra como os reguladores estão atentos a práticas que, embora sutis, têm um impacto significativo na proteção dos dados pessoais e na preservação da privacidade dos consumidores. Essas medidas reforçam a importância de um *design* ético de interfaces, que respeite a autonomia dos usuários e promova decisões verdadeiramente informadas.¹⁷⁸

Em resumo, as legislações e regulamentações ao redor do mundo têm evoluído para reconhecer e combater os *dark patterns* como práticas abusivas que comprometem a autonomia e a capacidade de decisão dos consumidores. Nos Estados Unidos, a FTC lidera esse combate com ações diretas e campanhas

¹⁷⁶ DEUTSCHLAND. *Bundesanstalt für Finanzdienstleistungsaufsicht*. BaFin: Dark Patterns in Trading Apps unzulässig. Disponível em: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2022/meldung_2022_11_21_Dark_Patterns_in_TradingApps_Experten.html. Acesso em: 10 ago. 2024.

¹⁷⁷ BATOCCHIO, Amália. *Guia nº 3/2022 da EDPB e a discussão sobre dark patterns*. Consultor Jurídico, 5 jul. 2022. Disponível em: <https://www.conjur.com.br/2022-jul-05/direito-digital-guia-32022-edpb-discussao-dark-patterns>. Acesso em: 10 ago. 2024.

¹⁷⁸ ITALIA. *Garante per la Protezione dei Dati Personali*. Newsletter 17/04/23 – Marketing: Garante privacy, no all'uso di modalità ingannevoli. Disponível em: <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870725>. Acesso em: 08 ago. 2024.

educativas, enquanto na União Europeia, o Regulamento de Serviços Digitais estabelece uma base legal sólida para proteger os consumidores em todo o continente. Essas iniciativas, combinadas com a crescente aplicação das leis em países como França, Alemanha e Itália, indicam um movimento global em direção a uma regulamentação mais rigorosa e eficaz contra *dark patterns*, promovendo um ambiente digital mais justo e transparente.

As legislações estrangeiras demonstram avanços significativos no combate aos *dark patterns*, mas, além dessas normas, é fundamental examinar como essas práticas manipulativas afetam diretamente a privacidade e a autonomia dos consumidores. Ao explorar o impacto dos *dark patterns* no comércio eletrônico, é importante entender como essas práticas podem enfraquecer a capacidade dos consumidores de tomar decisões informadas, colocando em risco tanto sua privacidade quanto sua liberdade de escolha.

2.3 PRIVACIDADE E AUTONOMIA DO CONSUMIDOR: CONCEITOS NECESSÁRIOS E FRAGILIZAÇÃO DIANTE DOS *DARK PATTERNS* NO COMÉRCIO ELETRÔNICO

A autonomia e a privacidade no ambiente digital são conceitos interconectados e fundamentais para a proteção do consumidor nesse espaço. Historicamente, a privacidade estava relacionada à proteção contra a interferência do Estado na vida privada, mas com o avanço das tecnologias da informação, esse conceito evoluiu para incluir a proteção dos dados pessoais e a preservação da identidade no meio digital. Conforme estabelecido no artigo 5º, inciso X, da Constituição Federal, a intimidade, a vida privada, a honra e a imagem das pessoas são invioláveis, garantindo-se o direito à indenização em caso de danos materiais ou morais resultantes de sua violação. Esse princípio constitucional reforça a necessidade de proteger a privacidade, especialmente num cenário onde as informações pessoais estão cada vez mais expostas e vulneráveis.¹⁷⁹

O conceito de autonomia do consumidor deve ser entendido como um processo contínuo e dinâmico, influenciado por diversos fatores, incluindo as interações com tecnologias digitais. Scherhorn defende que a autonomia é um processo em constante

¹⁷⁹ BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 09 ago. 2024.

evolução, e que os consumidores precisam desenvolver habilidades para resistir às influências externas que buscam direcionar seu comportamento.¹⁸⁰ Flusser sugere que, para exercer a autonomia, as pessoas precisam entender como funcionam os sistemas digitais. No entanto, a complexidade dos códigos binários e a centralização das infraestruturas digitais nas mãos de um pequeno grupo de corporações transnacionais limitam a capacidade dos consumidores de entender e controlar totalmente suas interações digitais. Isso resulta em um contexto onde o exercício da autonomia decisória é restrito, colocando em risco tanto a privacidade quanto a autonomia dos indivíduos em ambientes digitais dominados por grandes empresas tecnológicas.¹⁸¹

No entanto, no ambiente digital, os algoritmos de busca e as redes sociais têm um papel crescente na formação das preferências dos consumidores. Esses algoritmos influenciam as escolhas dos usuários, potencialmente limitando sua autonomia nas decisões. Bakshy *et al.* observam que, apesar das plataformas digitais oferecerem uma vasta gama de informações, os algoritmos tendem a priorizar conteúdos que confirmam as preferências e crenças já existentes dos usuários, restringindo o acesso a opiniões divergentes.¹⁸²

Isso levanta questões sobre a capacidade dos consumidores de exercerem plenamente sua autonomia em um ambiente onde as preferências são, em grande parte, moldadas por tecnologias que operam de maneira pouco transparente. Essa preocupação é ampliada por Wagner e Eidenmüller, que apontam que esses algoritmos são intencionalmente projetados para explorar vieses e moldar preferências, o que pode levar a uma diminuição significativa da autonomia do consumidor.¹⁸³

A economia digital, fundamentada na coleta e análise de dados pessoais, apresenta desafios significativos para a privacidade e a autonomia dos consumidores. Empresas utilizam tecnologias como *cookies* para rastrear o comportamento *on-line* dos usuários, criando perfis detalhados que são, em seguida, comercializados.

¹⁸⁰ SCHERHORN, G. The goal of consumer advice: Transparency or autonomy? *Journal of Consumer Policy*, v. 8, n. 2, p. 133-151, 1985.

¹⁸¹ FLUSSER, V. *Filosofia da caixa preta: ensaios para uma futura filosofia da fotografia*. Relume Dumará, 2002.

¹⁸² BAKSHY, Eytan; MESSING, Solomon; ADAMIC, Lada A. *Exposure to ideologically diverse news and opinion on Facebook*. *Science*, v. 348, n. 6239, p. 1130-1132, 2015.

¹⁸³ WAGNER, G.; EIDENMÜLLER, H. *Down by algorithms? Siphoning rents, exploiting biases, and shaping preferences: Regulating the dark side of personalized transactions*. *University of Chicago Law Review*, v. 86, n. 2, p. 581-609, 2019.

Silveira afirma que essa prática configura uma "economia da intrusão", onde os dados pessoais são monetizados sem o consentimento explícito e informado dos consumidores, comprometendo sua privacidade e, por consequência, sua autonomia.¹⁸⁴ Esse fenômeno é visto como um dos maiores desafios para a preservação da autonomia dos consumidores na era digital, como também destacado por Bjorlo, Moen e Pasquine, que ressaltam que, embora a personalização possa aumentar a satisfação do consumidor, ela também pode reduzir a diversidade das opções, levando os consumidores a optarem por produtos ou serviços que inicialmente não considerariam.¹⁸⁵

Além disso, a falta de controle efetivo dos consumidores sobre o uso de seus dados pessoais ameaça a própria democracia, uma vez que a privacidade é fundamental para o exercício da cidadania. Doneda destaca que, em muitas jurisdições, a proteção dos dados pessoais é vista como um direito fundamental, essencial para a defesa da dignidade humana. No entanto, a velocidade com que as tecnologias evoluem frequentemente supera a capacidade dos governos de regulamentar essas práticas adequadamente, deixando os consumidores expostos a abusos.¹⁸⁶

Essa realidade é agravada pelo controle excessivo exercido por sistemas de recomendação e algoritmos personalizados, que, segundo Mik, podem tanto aumentar quanto diminuir a autonomia do consumidor, dependendo da forma como são implementados. Quando a tecnologia interfere na capacidade do consumidor de fazer escolhas informadas e impõe preferências, a autonomia é comprometida, criando um ciclo vicioso de manipulação e restrição de escolhas.¹⁸⁷

A literatura reconhece amplamente a necessidade de mecanismos regulatórios para proteger a autonomia do consumidor em ambientes digitais. Kotliar destaca que, embora os algoritmos tenham o poder de influenciar as decisões dos consumidores, eles não são completamente autônomos ou imparciais, já que refletem os interesses daqueles que os desenvolvem e operam. Portanto, é essencial que intervenções

¹⁸⁴ SILVEIRA, Sérgio Amadeu. *Economia da intrusão e modulação na Internet. Liinc em Revista*, v. 12, n. 1, 2016. p. 21.

¹⁸⁵ BJORLO, L.; MOEN.; PASQUINE, M. *The role of consumer autonomy in developing sustainable AI: A conceptual framework*. Sustainability (Switzerland), v. 13, n. 4, p. 1-18, 2021. DOI: 10.3390/su13042332. Acesso em: 11 ago. 2024.

¹⁸⁶ DONEDA, Danilo. *A proteção dos dados pessoais como um direito fundamental*. Espaço Jurídico, v. 12, n. 2, p. 91-108, 2011.

¹⁸⁷ MIK, E. *The erosion of autonomy in online consumer transactions*. Law, Innovation and Technology, v. 8, n. 1, p. 1-38, 2016.

regulatórias sejam implementadas para garantir que os consumidores possam preservar um nível aceitável de autonomia diante das novas tecnologias.¹⁸⁸

A privacidade e a autonomia do consumidor no ambiente digital são conceitos que se reforçam mutuamente, mas enfrentam desafios significativos diante do progresso tecnológico e da economia da informação. A proteção dos dados pessoais é essencial para garantir esses direitos fundamentais, enquanto a compreensão e o controle das tecnologias digitais são vitais para o exercício pleno da autonomia no contexto atual, conforme assegurado pelos direitos previstos constitucionalmente. A autonomia do consumidor deve ser vista como um processo contínuo, e a intervenção regulatória é necessária para garantir que as novas tecnologias não comprometam a liberdade e o direito de escolha dos indivíduos.

A autonomia do consumidor em ambientes digitais é profundamente fragilizada pelo uso dos *dark patterns* no comércio eletrônico. Por exemplo, uma prática comum é a adição automática de itens ao carrinho de compras sem o consentimento explícito do consumidor, ou a continuação automática de uma assinatura paga após um período de teste gratuito, sem a devida notificação ou com dificuldades exageradas para o cancelamento. Essas estratégias minam a capacidade do consumidor de exercer sua autonomia de maneira plena e informada, ao criar situações onde as escolhas parecem limitadas ou forçadas.¹⁸⁹

Esses *dark patterns* exploram as vulnerabilidades inerentes dos consumidores, manipulando decisões de forma invisível. A fragilidade da autonomia do consumidor se manifesta especialmente quando tais práticas levam o indivíduo a realizar compras ou assumir compromissos financeiros que não pretendia, gerando não apenas frustração, mas também consequências financeiras negativas, como o endividamento. Mathur *et al.* observam que os *dark patterns* podem levar os consumidores a gastar mais do que pretendiam, aproveitando-se de fraquezas psicológicas e comportamentais, como a impulsividade e o medo de perder uma oferta. A incapacidade de resistir a essas manipulações revela o quanto a autonomia do consumidor pode ser corroída em ambientes digitais onde as escolhas são

¹⁸⁸ KOTLIAR, D. M. *Who Gets to choose?* on the socio-algorithmic construction of choice. *Science Technology and Human Values*, v. 46, n. 2, p. 346-375, 2021.

¹⁸⁹ BRIGNULL, Harry. *Dark patterns: deception vs. honesty in UI design*. A List Apart, 2011. Disponível em: <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/>. Acesso em: 11 ago. 2024.

estrategicamente influenciadas para beneficiar as empresas, e não o consumidor.¹⁹⁰

Além da manipulação direta das decisões de compra, os *dark patterns* também comprometem a privacidade e o controle que o consumidor tem sobre suas próprias informações. Bösch *et al.* destacam que muitas dessas práticas incluem a coleta de dados pessoais de forma sutil, muitas vezes sem o consentimento informado do usuário. Por exemplo, ao manipular interfaces para tornar a aceitação de políticas de privacidade ou a concessão de permissões menos visíveis, as empresas conseguem coletar uma quantidade significativa de dados pessoais que são usados para personalizar ainda mais as manipulações futuras. Isso não só viola a privacidade do consumidor, mas também restringe sua capacidade de tomar decisões informadas, criando um ciclo vicioso onde a autonomia é cada vez mais limitada.¹⁹¹

A manipulação imposta pelos *dark patterns* gera um ambiente digital onde a autonomia do consumidor é sistematicamente enfraquecida. O comércio eletrônico, ao adotar essas práticas, transformam o ambiente de consumo em um espaço hostil, onde as escolhas do consumidor são direcionadas por forças ocultas, dificultando o exercício da autonomia de forma transparente e consciente. Em um mercado onde os consumidores acreditam estar no controle de suas decisões, os *dark patterns* criam uma ilusão de escolha, mascarando a realidade de que muitas dessas decisões foram previamente influenciadas para servir aos interesses comerciais das empresas.

A falta de regulação eficaz sobre essas práticas permite que os *dark patterns* continuem a proliferar, exacerbando o desequilíbrio de poder entre empresas e consumidores. Gray *et al.* argumentam que, em um ambiente digital amplamente desregulado, as empresas têm pouca motivação para cessar o uso de *dark patterns*, especialmente quando essas práticas se mostram tão efetivas na maximização dos lucros. A ausência de medidas regulatórias rigorosas e a falta de mecanismos de proteção para os consumidores deixam-nos à mercê de um mercado cada vez mais inclinado a explorar suas vulnerabilidades.

Diante da crescente fragilização da privacidade e da autonomia do consumidor

¹⁹⁰ MATHUR, Arunesh; ACAR, Gunes; FRIEDMAN, Michael J.; LUCHERINI, Elena; MAYER, Jonathan; CHETTY, Marshini; NARAYANAN, Arvind. *Dark patterns at scale: Findings from a crawl of 11K shopping websites*. Proceedings of the ACM on Human-Computer Interaction, v. 3, n. CSCW, p. 1-32, nov. 2019. Disponível em: <https://doi.org/10.1145/3359183>. Acesso em: 18 ago. 2024.

¹⁹¹ BÖSCH, Christoph; ERB, Benjamin; KARGL, Frank; KOPP, Henning; PFATTHEICHER, Stefan. *Tales from the dark side: privacy dark strategies and privacy dark patterns*. Proceedings on Privacy Enhancing Technologies, v. 2016, n. 4, p. 237-254, out. 2016. Disponível em: <https://www.sciendo.com/article/10.1515/popets-2016-0038>. Acesso em: 18 ago. 2024.

no ambiente digital, exacerbada pelo uso de *dark patterns*, fica evidente a necessidade de intervenções que reequilibrem essa relação de poder. O cenário atual, onde as empresas utilizam técnicas manipulativas para maximizar lucros às custas dos consumidores, clama por diretrizes éticas e regulamentações mais robustas. Nesse contexto, surge a importância de explorar os princípios orientadores e diretrizes éticas estabelecidos pelo Guia nº 3/2022 da EDPB, que busca proporcionar uma estrutura sólida para proteger os direitos dos consumidores e garantir um ambiente digital mais transparente e justo.

2.4 PRINCÍPIOS ORIENTADORES E DIRETRIZES ÉTICAS DO GUIA Nº 3/2022 DA EDPB

O *European Data Protection Board (EDPB)*, preocupado com os impactos que os *dark patterns* podem ter na proteção de dados pessoais, emitiu em março de 2022 o Guia nº 3/2022, intitulado *Dark patterns in social media platform interfaces: How to recognise and avoid them*. Este guia oferece recomendações para que *designers* e usuários de plataformas de mídias sociais possam identificar e evitar a implementação de *dark patterns* que possam infringir a legislação de proteção de dados pessoais.¹⁹²

O Guia nº 3/2022 emitido pelo *European Data Protection Board (EDPB)* surge em um contexto de crescente preocupação com o uso de *dark patterns* nas interfaces das plataformas de mídias sociais e seus impactos na proteção de dados pessoais. Esses padrões obscuros, que manipulam as decisões dos usuários, têm o potencial de comprometer a privacidade e a autonomia informativa, princípios centrais da legislação europeia de proteção de dados, como a *General Data Protection Regulation (GDPR)*.

O Guia nº 3/2022 do EDPB define os *dark patterns* como "interfaces e experiências de usuário implementadas em plataformas de mídia social que levam os usuários a tomar decisões não intencionais, relutantes e potencialmente prejudiciais

¹⁹² EDPB. European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*. 21 de março de 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024.

sobre o processamento de seus dados pessoais"¹⁹³. Essa definição destaca a abordagem da autoridade europeia em relação ao tema, sinalizando como essas práticas podem violar princípios fundamentais da legislação de proteção de dados, como o consentimento informado e a transparência.¹⁹⁴

O guia europeu enumera seis tipos principais de *dark patterns*: (1) *Overloading*, onde o usuário é confrontado com uma grande quantidade de informações e opções, induzindo-o a compartilhar mais dados; (2) *Skipping*, que projeta a interface de modo que o usuário esqueça ou negligencie a proteção de dados; (3) *Stirring*, que manipula as escolhas dos usuários por meio de apelos emocionais ou visuais; (4) *Hindering*, que bloqueia ou dificulta a gestão de dados pessoais; (5) *Fickle*, que utiliza design inconsistente, dificultando a navegação do usuário; e (6) *Left in the dark*, que oculta informações ou ferramentas de controle de proteção de dados.¹⁹⁵

A importância do Guia nº 3/2022 é evidente ao demonstrar a preocupação das autoridades europeias em regular práticas que, apesar de não serem mencionadas explicitamente na GDPR, já eram abordadas em seus princípios gerais, como a proteção de dados por padrão e o consentimento livre e informado. A legislação europeia de proteção de dados, a *General Data Protection Regulation (GDPR)*, prevê, por exemplo, que a ativação por padrão de recursos invasivos de coleta de dados pode violar o princípio da "proteção de dados por padrão" (GDPR, art. 25). O Guia nº 3/2022 do EDPB, portanto, serve como uma ferramenta essencial para garantir que as plataformas digitais cumpram esses princípios ao longo de todo o ciclo de vida da conta do usuário.¹⁹⁶

¹⁹³ EDPB. European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces*: How to recognise and avoid them. 21 de março de 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024. p. 2.

¹⁹⁴ MATHUR, Arunesh; MAYER, Jonathan; KSHIRSAGAR, Mihir. *What Makes a Dark Pattern... Dark?* Design Attributes, Normative Considerations, and Measurement Methods. In: CHI Conference on Human Factors in Computing Systems (CHI '21), 8 a 13 de maio, 2021, Yokohama, Japan. New York: ACM, 2021. Disponível em: <https://arxiv.org/pdf/2101.04843.pdf>. Acesso em: 15 ago. 2024.

¹⁹⁵ EDPB. European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces*: How to recognise and avoid them. 21 de março de 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024. p. 2.

¹⁹⁶ EDPB. European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces*: How to recognise and avoid them. 21 de março de 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024.

No que tange aos princípios norteadores, vale destacar o princípio da transparência é central na proteção de dados, conforme destacado no artigo 5(1)(a) do GDPR. Este princípio exige que o processamento de dados pessoais seja feito de forma clara e acessível, possibilitando que os titulares compreendam como seus dados estão sendo utilizados e mantenham controle sobre eles. A transparência está profundamente conectada à justiça no tratamento de dados, pois a falta de informações adequadas ou informações enganosas pode levar a práticas desleais e à violação dos direitos dos titulares.¹⁹⁷

Outro princípio importante, conforme delineado nas diretrizes do Guia nº 3/2022 da EDPB, é a proteção de dados desde a concepção e por padrão. Este princípio, previsto no artigo 25 do GDPR, exige que os controladores adotem medidas técnicas e organizacionais apropriadas desde a criação de sistemas e serviços, garantindo que, por padrão, apenas os dados pessoais necessários para cada finalidade específica sejam processados.¹⁹⁸

As diretrizes do EDPB também sublinham a responsabilidade dos controladores de dados, ressaltando que eles devem demonstrar conformidade com todos os princípios do GDPR. Isso inclui a documentação apropriada dos processos de coleta e uso de dados, bem como a implementação de medidas que assegurem o cumprimento das normas de proteção de dados. A minimização de dados é outro princípio crucial, estipulando que apenas os dados pessoais estritamente necessários para alcançar os objetivos específicos do processamento devem ser coletados e tratados. Este princípio está relacionado à limitação da finalidade, que determina que os dados sejam processados exclusivamente para os fins declarados e legítimos.¹⁹⁹

As diretrizes éticas sugeridas pelo EDPB também reforçam a importância da

¹⁹⁷ EDPB. European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*. 21 de março de 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024.

¹⁹⁸ EDPB. European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*. 21 de março de 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024. p. 10.

¹⁹⁹ EDPB. European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them*. 21 de março de 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024. p. 10.

autonomia do titular dos dados, garantindo que ele tenha o maior controle possível sobre o uso e o processamento de suas informações pessoais. Isso inclui a capacidade de alterar configurações de privacidade de maneira simples e intuitiva, respeitando as expectativas razoáveis dos titulares.²⁰⁰

O EDPB destaca a necessidade de evitar o uso de *dark patterns* em interfaces de plataformas de mídias sociais, que podem induzir os usuários a tomar decisões não intencionais ou prejudiciais em relação ao tratamento de seus dados pessoais. Esses padrões escuros podem comprometer a capacidade dos usuários de proteger seus dados de forma eficaz e tomar decisões informadas.²⁰¹

No contexto brasileiro, embora a Lei Geral de Proteção de Dados (LGPD) não mencione expressamente os *dark patterns*, os princípios previstos no art. 6º da LGPD, como o da transparência e o da autodeterminação informativa, podem ser invocados contra práticas que prejudiquem os titulares de dados. O Guia nº 3/2022 do EDPB, portanto, não apenas reflete as preocupações europeias, mas também oferece uma base para discussões similares no Brasil, mostrando que práticas manipuladoras devem ser combatidas em todos os lugares.

O Guia nº 3/2022 do EDPB não só reflete a preocupação das autoridades europeias em regular práticas potencialmente danosas, mas também oferece uma base sólida para que outras jurisdições, como o Brasil, possam considerar diretrizes semelhantes. A Lei Geral de Proteção de Dados (LGPD), apesar de não mencionar expressamente os *dark patterns*, compartilha princípios que visam proteger os direitos dos titulares de dados contra práticas manipuladoras. Assim, o guia do EDPB serve como um alerta e um modelo para a proteção dos direitos dos usuários em um cenário global de crescente digitalização e coleta de dados. Ao promover a transparência e a autonomia dos usuários, o guia contribui para a construção de um ambiente digital mais justo e respeitoso, onde as decisões dos indivíduos sobre seus dados pessoais sejam verdadeiramente livres e informadas.

²⁰⁰ EDPB. European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces*: How to recognise and avoid them. 21 de março de 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024. p. 11.

²⁰¹ EDPB. European Data Protection Board. *Guidelines 3/2022 on Dark patterns in social media platform interfaces*: How to recognise and avoid them. 21 de março de 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024. p. 11.

3 IMPACTOS DO DESENVOLVIMENTO DE FERRAMENTAS DE DESIGN PARA MANIPULAÇÃO DA INFORMAÇÃO NO COMÉRCIO ELETRÔNICO: PROTEÇÃO AO CONSUMIDOR E MERCADO

O presente capítulo aborda os impactos do desenvolvimento de ferramentas de design utilizadas para manipulação da informação no comércio eletrônico, focalizando como essas tecnologias afetam a autodeterminação informativa e a capacidade de escolha consciente do consumidor. Serão analisadas as consequências do uso de *dark patterns* sob a perspectiva de regulamentações recentes, como o *Digital Market Act* e o *Digital Services Act (DSA)*, e seus reflexos na proteção de dados. Além disso, o capítulo examinará os marcos legais nacionais e internacionais voltados à proteção do consumidor no ambiente digital, oferecendo uma análise comparativa entre a legislação brasileira e as disposições do *Digital Market Act*, evidenciando os desafios e avanços na garantia dos direitos dos consumidores frente a práticas manipulativas em plataformas digitais.

3.1 IMPACTOS DO DESENVOLVIMENTO DE FERRAMENTAS DE DESIGN PARA MANIPULAÇÃO DA INFORMAÇÃO NA AUTODETERMINAÇÃO INFORMATIVA

O desenvolvimento de ferramentas de *design* voltadas para a manipulação informacional no comércio eletrônico tem gerado preocupações sobre o impacto na autodeterminação informativa dos consumidores. Esse conceito, fundamental para a proteção dos direitos da personalidade, assegura que o indivíduo mantenha controle sobre suas informações pessoais, inclusive no ambiente digital. No entanto, práticas como os *dark patterns* têm ameaçado essa autonomia, interferindo na capacidade dos consumidores de tomar decisões informadas. No cenário do comércio eletrônico, onde as interações e decisões são cada vez mais mediadas por interfaces digitais, a manipulação da informação por meio dessas ferramentas de *design* torna-se uma questão crítica para a manutenção da liberdade e da privacidade dos consumidores.

O direito à autodeterminação informativa é um conceito essencial na proteção dos direitos da personalidade, desenvolvido amplamente pelo Tribunal Constitucional Federal Alemão. Inicialmente, esse direito era visto como uma liberdade geral de ação, permitindo que o indivíduo tomasse decisões sobre sua própria vida. No entanto, com o tempo, essa interpretação foi expandida para incluir a proteção da

esfera privada, assegurando ao indivíduo proteção contra interferências indevidas de terceiros, especialmente no que diz respeito às suas informações pessoais.²⁰²

A decisão histórica do Tribunal Alemão sobre a Lei do Censo de 1983 definiu claramente o direito à autodeterminação informativa, afirmando que ele consiste no poder do indivíduo de decidir por si próprio, quando e dentro de que limites suas informações pessoais serão reveladas.²⁰³ Esse direito vai além da simples proteção contra o acesso não autorizado às informações; ele se estende a todas as fases de processamento de dados, garantindo que o controle sobre as informações pessoais seja mantido pelo indivíduo.

Com o avanço das tecnologias e das práticas comerciais no ambiente digital, novas ameaças à autodeterminação informativa têm surgido, particularmente no contexto do comércio eletrônico. O desenvolvimento de ferramentas de design conhecidas como *dark patterns* tem gerado impactos significativos na manipulação da informação, comprometendo a capacidade dos consumidores de tomar decisões informadas e racionais.²⁰⁴ Essas práticas de *design* são voltadas para influenciar ou manipular as escolhas dos consumidores, beneficiando as empresas e restringindo a autonomia dos usuários.

Os *dark patterns* afetam diretamente a autonomia dos consumidores ao dificultarem o processo de tomada de decisão. Exemplos dessas práticas incluem a imposição de ações forçadas ou a criação de obstáculos para o cancelamento de serviços, demonstrando como essas ferramentas são usadas para manipular o comportamento dos consumidores, impedindo-os de fazer escolhas que realmente desejam.²⁰⁵ Essas barreiras intencionalmente criadas complicam a realização de escolhas informadas, ameaçando a autodeterminação informativa e infringindo os direitos dos consumidores.

Além disso, as estratégias de *dark patterns* frequentemente exploram vulnerabilidades cognitivas dos consumidores, interferindo em seu processo

²⁰² MENDES, Laura S. F. *Autodeterminação informativa: a história de um conceito*. Pensar: Revista de Ciências Jurídicas, v. 25, n. 4, p. 34-58, out./dez. 2020. p. 12.

²⁰³ SCHWABE, Jürgen; MARTINS, Leonardo. *Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão*. Montevideo: Konrad Adenauer Stiftung, 2005. p. 237.

²⁰⁴ FRAZÃO, Ana. *Como conter as dark patterns*. Jota, 12 jun. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/como-conter-as-dark-patterns>. Acesso em: 08 set. 2024.

²⁰⁵ FRAZÃO, Ana. *Como conter as dark patterns*. Jota, 12 jun. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/como-conter-as-dark-patterns>. Acesso em: 08 set. 2024.

decisório. Um exemplo clássico dessas práticas é a pré-seleção de opções que favorecem a empresa, induzindo o consumidor a uma decisão automática que pode não refletir seus verdadeiros interesses. A vulnerabilidade informacional dos consumidores é exacerbada pela assimetria de poder no ambiente digital, onde as empresas utilizam os dados pessoais dos consumidores para moldar suas experiências *on-line*, comprometendo tanto a privacidade quanto a liberdade de escolha.²⁰⁶

Outro impacto significativo dos *dark patterns* é o uso de informações falsas ou enganosas para influenciar as decisões dos consumidores. Práticas como criar uma falsa sensação de urgência ou disfarçar publicidade são tentativas deliberadas de enganar o consumidor, levando-o a acreditar que suas decisões são baseadas em fatos, quando na verdade estão sendo manipuladas para favorecer a empresa.²⁰⁷ Isso compromete a integridade do processo decisório e viola o direito do consumidor de ser adequadamente informado, prejudicando sua capacidade de tomar decisões autônomas.

No contexto do comércio eletrônico, onde as decisões de compra são frequentemente rápidas e baseadas em informações visuais, os *dark patterns* tornam-se ainda mais perigosos. A manipulação na apresentação das informações, como ocultar dados importantes ou dificultar comparações, pode levar o consumidor a fazer escolhas que não faria se estivesse totalmente informado.²⁰⁸ Essa manipulação digital não apenas infringe a autodeterminação informativa, mas também pode resultar em decisões de compra prejudiciais, criando um ambiente onde o consumidor perde o controle sobre suas próprias escolhas.

A aplicação de *dark patterns* no comércio eletrônico tem criado um cenário em que os consumidores gradualmente perdem o controle sobre suas próprias decisões. A complexidade e a sofisticação dessas ferramentas de *design* criam uma falsa impressão de escolha, quando na realidade as opções são cuidadosamente manipuladas para conduzir a uma decisão pré-determinada.

²⁰⁶ ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova estrutura do poder. Intrínseca, 2020. p. 45.

²⁰⁷ FRAZÃO, Ana. *Como conter as dark patterns*. Jota, 12 jun. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/como-conter-as-dark-patterns>. Acesso em: 08 set. 2024.

²⁰⁸ FRAZÃO, Ana. *Como conter as dark patterns*. Jota, 12 jun. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/como-conter-as-dark-patterns>. Acesso em: 08 set. 2024.

Para mitigar os impactos dos *dark patterns* na autodeterminação informativa, é crucial que o ordenamento jurídico brasileiro seja rigorosamente aplicado. Tanto o Código de Defesa do Consumidor (CDC) quanto a Lei Geral de Proteção de Dados (LGPD) oferecem uma base sólida para proteger os consumidores contra essas práticas manipulativas.²⁰⁹ No entanto, a efetividade dessas leis depende de uma aplicação consistente e de um maior conhecimento dos consumidores sobre seus direitos, destacando a importância da educação digital.

A proteção contra *dark patterns* não se limita à aplicação das leis existentes, mas também envolve a conscientização dos consumidores sobre essas práticas enganosas. Educar os consumidores sobre como essas ferramentas de *design* operam e como podem influenciar suas decisões de compra é essencial para que possam tomar decisões mais informadas e evitar armadilhas digitais.²¹⁰

Os desafios impostos pelos *dark patterns* também ressaltam a importância da transparência e da ética no *design* de interfaces digitais. As empresas precisam ser responsabilizadas por práticas que buscam manipular o comportamento dos consumidores de maneira injusta. Promover práticas de *design* transparentes e que respeitem a autodeterminação informativa é essencial para garantir um ambiente de comércio eletrônico justo e confiável, o que requer uma abordagem mais rigorosa por parte das autoridades reguladoras.

Rodotá defende que a proteção de dados pessoais deve ser entendida não apenas como uma questão individual, mas também como uma responsabilidade coletiva, exigindo a colaboração entre consumidores, empresas e autoridades reguladoras.²¹¹ Essa abordagem colaborativa é fundamental para fortalecer a autodeterminação informativa no ambiente digital.

A falta de transparência no uso de *dark patterns* agrava ainda mais a vulnerabilidade algorítmica dos consumidores, criando um abismo informacional que dificulta o pleno exercício da autodeterminação informativa.²¹² Essa manipulação

²⁰⁹ FRAZÃO, Ana. *Como conter as dark patterns*. Jota, 12 jun. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/como-conter-as-dark-patterns>. Acesso em: 08 set. 2024.

²¹⁰ FRAZÃO, Ana. *Como conter as dark patterns*. Jota, 12 jun. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/como-conter-as-dark-patterns>. Acesso em: 08 set. 2024.

²¹¹ RODOTÁ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização de Maria Celina Bodin de Moraes. Tradução: Danilo Doneada e Luciana Cabral Doneada. Rio de Janeiro: Renovar, 2008. p. 50.

²¹² NISSENBAUM, Helen. *Privacy as contextual integrity*. *Washington Law Review*, v. 79, p. 119-158,

digital destaca a necessidade de regras claras de fluxo de informações para proteger valores sociais como a liberdade, a autonomia e a igualdade informacional.

A proteção contra *dark patterns* deve ir além do mero consentimento do usuário, exigindo uma análise mais ampla das circunstâncias e do contexto em que essas práticas ocorrem.²¹³ Isso inclui a consideração dos impactos negativos sobre a autodeterminação informativa e a necessidade de mecanismos que garantam transparência e controle aos consumidores sobre suas informações. A abordagem de Bioni enfatiza a importância de equilibrar os interesses econômicos das empresas com os direitos fundamentais dos consumidores.

Os *dark patterns*, ao comprometerem a integridade contextual da privacidade e manipularem as decisões dos consumidores, violam esse direito e contribuem para a perpetuação de um mercado desequilibrado, onde o poder está concentrado nas mãos das grandes plataformas digitais. A implementação de medidas como o *opt-out* e a introdução de salvaguardas é fundamental para proteger a autodeterminação informativa e evitar a criação de um estado de danosidade para os usuários.²¹⁴

No contexto do comércio eletrônico, o uso intensivo de *dark patterns* destaca a fragilidade do consumidor digital diante das estratégias de manipulação informacional. Conforme observado por Verbicaro e Calandrini, a aplicação dessas técnicas deve ser rigorosamente regulamentada para garantir que o legítimo interesse das empresas não se sobreponha aos direitos dos consumidores. A ausência de regulamentação adequada permite que as empresas explorem as assimetrias de informação em benefício próprio, em detrimento dos direitos dos consumidores.²¹⁵

Além das regulamentações, a implementação de medidas de *privacy by design* é fundamental para mitigar os impactos negativos dos *dark patterns* no comércio eletrônico. Essa abordagem propõe a incorporação de princípios de privacidade desde o início do processo de *design*, garantindo que as interfaces digitais sejam desenvolvidas de forma a respeitar a autodeterminação informativa e proteger os

2004. Disponível em: <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>. Acesso em: 07 set. 2024. p. 128.

²¹³ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020. p. 198.

²¹⁴ MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. *Proteção de dados para além do consentimento: tendências contemporâneas de materialização*. Revista Estudos Institucionais, Rio de Janeiro, v. 6, n. 2, p. 507-533, maio/ago. 2020. p. 519.

²¹⁵ VERBICARO, Dennis; CALANDRINI, Jorge. *A proteção da confiança do consumidor e a base do legítimo interesse na lei nº 13.709/2018* (Lei Geral de Proteção de Dados Pessoais). Revista de Direito do Consumidor, vol. 139/2022, p. 73-99, jan.-fev., 2022. p. 87.

direitos dos consumidores.²¹⁶ A adoção dessa metodologia pode ajudar a reequilibrar a relação de poder no ambiente digital.

A flexibilidade do conceito de autodeterminação informativa permite sua aplicação em uma ampla variedade de situações relacionadas ao tratamento de dados pessoais. Essa adaptabilidade é essencial para enfrentar os desafios impostos pelo avanço tecnológico e pela crescente complexidade das operações de processamento de dados na era digital. O direito à autodeterminação informativa é, portanto, um direito dinâmico que se adapta às novas realidades impostas pelas mudanças sociais e tecnológicas. Sua relevância no contexto do comércio eletrônico é evidente, pois garante que o indivíduo mantenha o controle sobre suas informações pessoais, enfrentando os desafios contemporâneos trazidos pela digitalização e pelo processamento massivo de dados.²¹⁷

A manipulação informacional por meio de *dark patterns* representa uma séria ameaça à autodeterminação informativa, uma vez que esses padrões de design são criados para explorar as vulnerabilidades dos consumidores e orientar suas escolhas de maneira que favoreça os interesses corporativos. A utilização de algoritmos para personalizar a navegação e as ofertas comerciais cria um ambiente em que as escolhas dos consumidores são pré-definidas, limitando sua liberdade de decisão e exacerbando a vulnerabilidade informacional.²¹⁸

A integridade contextual da privacidade, como argumentado por Nissenbaum, é essencial na proteção contra a vigilância pública e a manipulação informacional. Entretanto, a adoção de *dark patterns* no *design* de interfaces digitais infringe esse princípio ao distorcer o fluxo de informações e induzir os consumidores a tomar decisões que contrariam seus próprios interesses. Isso reforça a necessidade de uma regulamentação mais rigorosa e de uma arquitetura normativa que proteja a integridade informacional dos consumidores, garantindo que suas expectativas de privacidade sejam respeitadas.²¹⁹

²¹⁶ COTS, Márcio; OLIVEIRA, Ricardo de (Coord.). *O legítimo interesse e a LGPD*. São Paulo: Revista dos Tribunais, 2020. p. 153.

²¹⁷ ROUVROY, Antoinette; POULLET, Yves. *The right to informational self-determination and the value of self-development*. In: GUTWIRTH, S. et al. (Ed.). *Reinventing data protection?* Dordrecht: Springer, 2009. p. 10.

²¹⁸ MILHOMENS, Heitor Antunes. *Tutela da confiança e da vulnerabilidade na economia do compartilhamento: empoderamento do consumidor digital e mitigação da vulnerabilidade estrutural na era do hiperconsumo*. 2021. Dissertação (Mestrado em Direito) — Universidade Federal do Pará, Belém, 2021. p. 202.

²¹⁹ NISSENBAUM, Helen. *Privacy as contextual integrity*. *Washington Law Review*, v. 79, p. 119-158, 2004. Disponível em: <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>. Acesso em: 07 set. 2024.

A manipulação informacional por meio de *dark patterns* também levanta profundas questões éticas no contexto do comércio eletrônico. Como discutido por Verbicaro e Vieira, a coleta e o tratamento indevidos dos dados pessoais dos consumidores por meio dessas técnicas constituem uma violação direta dos direitos da personalidade, incluindo a privacidade e a intimidade.²²⁰ Além disso, tais práticas alimentam um ambiente de consumo caracterizado pela desigualdade e exploração, onde as escolhas dos consumidores são direcionadas para beneficiar exclusivamente as empresas.

A vulnerabilidade informacional dos consumidores, resultado direto da assimetria de poder no ambiente digital, é exacerbada pelo uso de *dark patterns*. Essas práticas manipulativas criam um "microcosmo" informacional, como descrito por Zuboff, que condiciona as interações dos consumidores no ciberespaço, limitando suas opções e comprometendo sua autodeterminação informativa.²²¹ Em um ambiente onde as decisões de compra são frequentemente rápidas e baseadas em informações visuais, os consumidores ficam ainda mais expostos a essas manipulações.

Para proteger os consumidores, é essencial que a autodeterminação informativa seja mantida como um direito imprescindível e que as práticas de *dark patterns* sejam rigorosamente fiscalizadas e regulamentadas. Isso inclui a implementação de medidas que garantam transparência e controle aos consumidores sobre suas informações.²²² A conscientização sobre o funcionamento dessas ferramentas de *design* e sobre como elas podem influenciar as decisões de compra dos consumidores é essencial para promover um ambiente de consumo mais equilibrado. Além disso, a transparência e a ética no *design* de interfaces digitais são fundamentais para garantir que os consumidores possam exercer plenamente sua autodeterminação informativa.

Nesse sentido, a proteção contra *dark patterns* deve ser entendida como um aspecto central na defesa da autodeterminação informativa. A implementação de uma regulamentação eficaz, aliada à educação digital e à promoção de práticas de design

²²⁰ VERBICARO, Dennis; CALANDRINI, Jorge. *A proteção da confiança do consumidor e a base do legítimo interesse na lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais)*. Revista de Direito do Consumidor, vol. 139/2022, p. 73-99, jan.-fev., 2022.

²²¹ ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova estrutura do poder*. Intrínseca, 2020. p. 45.

²²² BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020. p. 198.

éticas e transparentes, é imprescindível para assegurar que os consumidores possam tomar decisões informadas e autônomas no ambiente digital. A autodeterminação informativa, como um direito dinâmico, deve continuar a evoluir para enfrentar os desafios do avanço tecnológico e garantir a proteção dos direitos dos consumidores no comércio eletrônico.

Diante dos desafios impostos pelos *dark patterns* e suas implicações para a autodeterminação informativa, é essencial discutir o papel de regulamentações internacionais que buscam proteger os consumidores contra essas práticas. Normativas como o *Digital Market Act* e o *Digital Services Act (DSA)* têm emergido como respostas para conter os abusos de poder das grandes plataformas digitais e garantir a proteção de dados pessoais. Esses marcos regulatórios visam estabelecer um equilíbrio entre os interesses comerciais e os direitos fundamentais dos consumidores, criando um ambiente digital mais transparente e seguro.

3.2 DARK PATTERNS: DIGITAL MARKET ACT, DIGITAL SERVICES ACT (DSA) E SEUS IMPACTOS NA PROTEÇÃO DE DADOS

O desenvolvimento de regulamentações específicas para o mercado digital tem se mostrado cada vez mais necessário diante do crescente uso de práticas manipulativas, como os *dark patterns*. Nesse contexto, o *Digital Markets Act (DMA)* e o *Digital Services Act (DSA)* emergem como marcos importantes na União Europeia, buscando não apenas garantir uma maior transparência, mas também proteger os consumidores contra abusos de grandes plataformas digitais. Ao adotar medidas preventivas e sanções rigorosas, esses regulamentos pretendem restabelecer o equilíbrio de poder no ambiente digital, assegurando que os dados pessoais dos consumidores sejam tratados de maneira ética e que suas decisões não sejam manipuladas por interfaces projetadas para influenciar de forma enganosa suas escolhas.

O *Digital Markets Act (DMA)* surge em 2022 como um marco regulatório de grande relevância na Europa, criado pela União Europeia para responder à crescente concentração do mercado digital em poucas plataformas, conhecidas como *gatekeepers*, que detêm significativo poder de mercado. Essas plataformas exercem um controle profundo sobre o acesso à informação e impactam fortemente a concorrência, gerando preocupações sobre práticas anticoncorrenciais e o tratamento

dos dados pessoais dos usuários.²²³ Nesse contexto, o DMA busca regular preventivamente as atividades dessas grandes plataformas digitais, antes que práticas abusivas possam ocorrer, o que inclui a mitigação dos *dark patterns*, que têm sido amplamente criticados por comprometerem a transparência e a autonomia dos usuários.²²⁴

Esses padrões obscuros referem-se a estratégias manipulativas usadas por plataformas digitais para influenciar as escolhas dos consumidores, favorecendo os interesses comerciais dessas empresas. As práticas incluem desde a ocultação de opções de privacidade até a criação de obstáculos artificiais para o cancelamento de serviços. Tais estratégias dificultam a proteção dos dados pessoais e comprometem a transparência nas relações comerciais, pois muitas vezes os consumidores são levados a compartilhar mais informações do que desejam ou a manter serviços que não precisam.²²⁵ O DMA propõe uma abordagem mais rígida para reprimir essas práticas, introduzindo sanções para os *gatekeepers* que continuarem a adotar esses comportamentos.²²⁶

A regulação dos padrões obscuros pelo DMA é particularmente relevante no contexto atual, onde a coleta massiva de dados e o uso de algoritmos sofisticados aumentam as possibilidades de manipulação dos consumidores. Ao regular esses padrões, o DMA visa garantir um ambiente digital mais transparente e seguro, onde os direitos dos usuários são respeitados e protegidos.²²⁷

O DMA também se destaca por adotar uma regulação *ex ante*, ou seja, um conjunto de regras que as plataformas devem seguir antes de certas atividades ocorrerem, prevenindo abusos de poder de mercado. Essa regulação é essencial para evitar comportamentos que possam prejudicar a concorrência e a proteção de dados

²²³ CABRAL, Anna Cecília Moreira. *Digital Markets Act: porque uma regulação ex ante para plataformas?* Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 9, n. 1, p. 76–96, jan./jul. 2023. p. 79.

²²⁴ SANTOS, Humberto Cunha dos. *Digital Markets Act e suas implicações para a concorrência digital*. JOTA, 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/digital-markets-act-25112022>. Acesso em: 09 set. 2024.

²²⁵ CREMÉR, Jacques. *Competition policy for the digital era: A report commissioned by the European Commission*. 2019. Disponível em: <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>. Acesso em: 09 set. 2024.

²²⁶ FURMAN, Jason. *Unlocking digital competition: Report of the Digital Competition Expert Panel*. 2019. Disponível em: <https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel>. Acesso em: 09 set. 2024.

²²⁷ CABRAL, Anna Cecília Moreira. *Digital Markets Act: porque uma regulação ex ante para plataformas?* Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 9, n. 1, p. 76–96, jan./jul. 2023.

dos consumidores, garantindo que as plataformas atuem de maneira justa e transparente. Além disso, o DMA propõe a criação de uma nova Autoridade de Mercados Digitais, encarregada de monitorar o cumprimento das normas e aplicar sanções em caso de violações, o que reforça a eficácia dessa regulação preventiva.²²⁸ A criação dessa autoridade é uma das inovações mais importantes do DMA, fundamental para assegurar a efetividade da regulação em um mercado tão dinâmico.²²⁹

Um dos principais objetivos do DMA é regular a interação entre as plataformas *gatekeepers* e as empresas terceirizadas que utilizam seus serviços. Há preocupações de que os termos e condições impostos por essas plataformas possam prejudicar a concorrência e restringir a liberdade de escolha dos consumidores. O DMA busca assegurar que essas interações sejam justas e transparentes, promovendo um mercado mais equilibrado.²³⁰ A transparência nas interações comerciais e o acesso igualitário a dados e algoritmos são essenciais para manter a integridade e a competitividade do mercado digital.²³¹

A proteção de dados pessoais é outro aspecto fundamental abordado pelo DMA. O regulamento exige que as plataformas obtenham consentimento explícito dos usuários antes de coletar ou processar seus dados, proibindo o uso desses dados para publicidade direcionada sem a devida autorização. Essa medida visa proteger a privacidade dos usuários e garantir que seus dados não sejam usados de maneira abusiva.²³² A abordagem preventiva do DMA é necessária para assegurar que o uso de dados pessoais pelas plataformas seja ético e transparente, fortalecendo a confiança do público no ambiente digital.²³³

²²⁸ CABRAL, Anna Cecília Moreira. *Digital Markets Act: porque uma regulação ex ante para plataformas?* Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 9, n. 1, p. 76–96, jan./jul. 2023.

²²⁹ GERADIN, Damien. *What is a digital gatekeeper? Which platforms should be captured by the EC proposal for a digital market act?* SSRN, 2021. Disponível em: <https://ssrn.com/abstract=3853991>. Acesso em: 08 set. 2024.

²³⁰ CABRAL, Anna Cecília Moreira. *Digital Markets Act: porque uma regulação ex ante para plataformas?* Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 9, n. 1, p. 76–96, jan./jul. 2023.

²³¹ KERBER, Wolfgang. *Taming Tech Giants with a Per-Se Rules Approach?* The Digital Markets Act from the 'Rules vs. Standard' Perspective. *Taming tech giants with a per se rules approach*, p. 28-34, 2021. p. 34.

²³² CABRAL, Anna Cecília Moreira. *Digital Markets Act: porque uma regulação ex ante para plataformas?* Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 9, n. 1, p. 76–96, jan./jul. 2023.

²³³ HOVENKAMP, Herbert. *Antitrust and innovation: where we are and where we should be going*. *Antitrust Law Journal*, Connecticut, n. 77, p. 749-751, 2011. p. 749.

Além disso, o DMA estabelece critérios rigorosos para garantir a transparência das plataformas no uso de algoritmos. A preocupação é que esses algoritmos possam ser usados para manipular a classificação de produtos e serviços, favorecendo injustamente certas empresas ou produtos. O regulamento exige que os *gatekeepers* divulguem os algoritmos utilizados e expliquem as decisões de classificação que possam ser percebidas como discriminatórias, assegurando maior proteção contra vieses algorítmicos.²³⁴ A transparência na aplicação de algoritmos é essencial para prevenir práticas discriminatórias e garantir a equidade no mercado digital.²³⁵

A regulação *ex ante* também facilita a contestação por parte da sociedade e do Poder Público, uma vez que as obrigações impostas às plataformas estão claramente definidas no DMA. Isso permite maior fiscalização e intervenção para corrigir práticas inadequadas antes que causem danos significativos ao mercado ou aos consumidores. Outro ponto relevante é que o DMA busca evitar a fragmentação do mercado europeu, promovendo a uniformidade das regras aplicáveis a todas as plataformas digitais que operam na região. Isso é essencial para preservar o mercado transfronteiriço e garantir que as empresas possam competir em condições de igualdade, independentemente do país em que atuam.²³⁶

Casos anteriores ao DMA envolvendo a Google, que enfrentou multas substanciais por práticas anticoncorrenciais na União Europeia, ilustram a necessidade de uma regulação mais ampla e proativa. A aplicação *ex post* da lei mostrou-se ineficaz em muitos casos, levando a prejuízos para a concorrência e dificuldades na proteção de dados pessoais. O DMA busca corrigir essas falhas, estabelecendo regras claras a serem seguidas desde o início.²³⁷

A crescente adoção de táticas manipulativas no mercado digital evidenciou a necessidade urgente de reavaliar a estrutura de proteção ao consumidor na União Europeia. Mesmo na atualidade, é surpreendente que muitas plataformas de compras online ainda dependam de práticas enganosas para explorar as vulnerabilidades dos

²³⁴ CABRAL, Anna Cecília Moreira. *Digital Markets Act: porque uma regulação ex ante para plataformas?* Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 9, n. 1, p. 76–96, jan./jul. 2023.

²³⁵ BALDWIN, Robert; CAVE, Martin. *Understanding regulation: theory, strategy, and practice*. Oxford: Oxford University Press, 2011. p. 198.

²³⁶ CABRAL, Anna Cecília Moreira. *Digital Markets Act: porque uma regulação ex ante para plataformas?* Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 9, n. 1, p. 76–96, jan./jul. 2023.

²³⁷ CABRAL, Anna Cecília Moreira. *Digital Markets Act: porque uma regulação ex ante para plataformas?* Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 9, n. 1, p. 76–96, jan./jul. 2023.

consumidores ou enganá-los de forma deliberada.²³⁸ Esse fenômeno reflete uma preocupação econômica e social, onde as plataformas utilizam estratégias sofisticadas para influenciar as escolhas dos usuários, muitas vezes comprometendo sua autonomia. Essas práticas afetam diretamente a liberdade de escolha dos consumidores e levantam questões sobre a eficácia das regulamentações existentes para protegê-los dessas táticas predatórias.²³⁹

O *Digital Services Act (DSA)* também tem sido amplamente debatido, especialmente por sua abrangência, que inclui não apenas as grandes plataformas online, mas também todos os intermediários digitais. Isso abrange qualquer negócio que armazene ou transmita informações em nome de terceiros, ampliando significativamente o escopo da norma. A inclusão dos intermediários visa mitigar os riscos associados à manipulação de dados e ao uso de padrões obscuros, que podem levar os consumidores a tomar decisões que não refletem seus melhores interesses. Assim, o DSA busca garantir que as interações dos consumidores com as plataformas sejam mais transparentes, evitando que suas escolhas sejam manipuladas para favorecer interesses comerciais das plataformas.²⁴⁰

A proteção de dados e a privacidade no contexto digital são temas centrais nas discussões em torno do DMA e do DSA. Os padrões obscuros, ao induzirem os consumidores a fornecer dados pessoais de forma inconsciente ou involuntária, representam uma ameaça direta aos direitos de privacidade. A coleta e o uso de dados pessoais sem o devido consentimento informado violam as diretrizes do Regulamento Geral de Proteção de Dados (RGPD), que visa assegurar o controle dos consumidores sobre suas informações. A violação dessas normas não só prejudica os consumidores individualmente, mas também mina a confiança no ambiente digital, o que pode ter consequências negativas para o crescimento do mercado digital.²⁴¹

O RGPD desempenha um papel essencial na regulação dos padrões obscuros, particularmente na proteção da privacidade dos consumidores. Ao impor regras claras

²³⁸ OCDE. Dark commercial patterns. Digital Economy Papers, n. 336, OECD Publishing, Paris, 2022.

²³⁹ MELO JUNIOR, Glauto Lisboa. *Navegando por padrões obscuros: uma análise crítica da Lei dos Mercados Digitais (DMA) e da Lei dos Serviços Digitais (DSA) para a proteção dos consumidores online*. Revista da Faculdade de Direito da Universidade de Lisboa, Lisboa, v. 64, n. 2, p. 545-573, 2023.

²⁴⁰ MELO JUNIOR, Glauto Lisboa. *Navegando por padrões obscuros: uma análise crítica da Lei dos Mercados Digitais (DMA) e da Lei dos Serviços Digitais (DSA) para a proteção dos consumidores online*. Revista da Faculdade de Direito da Universidade de Lisboa, Lisboa, v. 64, n. 2, p. 545-573, 2023.

²⁴¹ MELO JUNIOR, Glauto Lisboa. *Navegando por padrões obscuros: uma análise crítica da Lei dos Mercados Digitais (DMA) e da Lei dos Serviços Digitais (DSA) para a proteção dos consumidores online*. Revista da Faculdade de Direito da Universidade de Lisboa, Lisboa, v. 64, n. 2, p. 545-573, 2023.

sobre o consentimento informado e a transparência nas práticas de tratamento de dados, o RGPD procura impedir que as empresas usem estratégias manipulativas para obter informações pessoais dos usuários sem seu pleno conhecimento. No entanto, a aplicação dessas regras enfrenta desafios, pois as empresas frequentemente criam interfaces que obscurecem as verdadeiras intenções por trás da coleta de dados, dificultando a detecção dessas práticas. Isso ressalta a necessidade de uma fiscalização mais rigorosa e de medidas adicionais para proteger efetivamente os direitos dos consumidores.²⁴²

Os legisladores do DSA decidiram limitar a proibição de táticas de *design* enganosas apenas às plataformas *on-line*, o que restringe o impacto da norma aos padrões obscuros em contextos específicos. Embora essa escolha seja relevante, ela reduz o alcance potencial do DSA, deixando outras áreas do mercado digital menos regulamentadas. Essa delimitação pode ser vista como uma estratégia para viabilizar a implementação da norma, mas também cria lacunas que podem ser exploradas por empresas que operam fora das grandes plataformas. Isso sublinha a necessidade de equilibrar a criação de regras aplicáveis com a proteção ampla de todos os consumidores, independentemente da plataforma que utilizem.²⁴³

As novas regulamentações, como o *Digital Markets Act (DMA)* e o *Digital Services Act (DSA)*, têm o potencial de influenciar práticas em mercados globais além das fronteiras da União Europeia. As empresas globais que operam na UE frequentemente adotam as normas europeias como padrão para suas operações em outras regiões, devido à complexidade e ao custo de adaptar suas práticas a diferentes regimes legais. Assim, as disposições do DMA e do DSA podem estabelecer um novo padrão global para a regulação do mercado digital, promovendo maior transparência e proteção ao consumidor em escala internacional. No entanto, a eficácia dessas normas dependerá de sua implementação prática e da capacidade das autoridades reguladoras de fiscalizar e aplicar as regras.²⁴⁴

Com a crescente acessibilidade aos dados e os avanços no *Big Data* e na

²⁴² MELO JUNIOR, Glauto Lisboa. *Navegando por padrões obscuros: uma análise crítica da Lei dos Mercados Digitais (DMA) e da Lei dos Serviços Digitais (DSA) para a proteção dos consumidores on-line*. Revista da Faculdade de Direito da Universidade de Lisboa, Lisboa, v. 64, n. 2, p. 545-573, 2023.

²⁴³ BURI, Ilaria; VAN HOBOKEN, Joris. *The Digital Services Act (DSA) proposal: a critical overview*. Digital Services Act (DSA) Observatory Institute for Information Law (IViR), Universidade de Amsterdã, 2021.

²⁴⁴ MELO JUNIOR, Glauto Lisboa. *Navegando por padrões obscuros: uma análise crítica da Lei dos Mercados Digitais (DMA) e da Lei dos Serviços Digitais (DSA) para a proteção dos consumidores on-line*. Revista da Faculdade de Direito da Universidade de Lisboa, Lisboa, v. 64, n. 2, p. 545-573, 2023.

Inteligência Artificial, os operadores do mercado digital têm refinado práticas que rastreiam e mapeiam o comportamento dos consumidores. Essas práticas, altamente detalhadas e personalizadas, permitem às empresas adquirir um conhecimento profundo sobre as preferências dos consumidores, o que pode ser usado tanto para melhorar a oferta de produtos quanto para explorar suas vulnerabilidades. Nesse contexto, o uso de padrões obscuros é especialmente preocupante, pois essas práticas sofisticadas podem manipular as decisões dos consumidores de maneiras difíceis de detectar e combater.²⁴⁵

Apesar das disposições do DSA, a definição precisa do que constitui um padrão obscuro ainda permanece nebulosa. Essa falta de clareza cria desafios significativos para a regulamentação e aplicação da lei, uma vez que as empresas podem explorar ambiguidades para continuar utilizando práticas manipulativas sem enfrentar consequências legais. A natureza dinâmica dos padrões obscuros, que se adaptam rapidamente às novas tecnologias e ao comportamento do consumidor, torna ainda mais difícil estabelecer uma definição clara e abrangente. Assim, a eficácia do DSA dependerá tanto da clareza das definições legais quanto da capacidade das autoridades reguladoras de identificar e agir contra essas práticas de forma proativa.²⁴⁶

No combate a algoritmos manipuladores, o DSA se destaca ao exigir que grandes plataformas e motores de busca identifiquem, analisem e avaliem diligentemente todos os riscos sistêmicos decorrentes do *design* ou funcionamento de seus serviços. O artigo 34.º do DSA é inovador ao estabelecer essa obrigação, que visa mitigar os efeitos negativos dos padrões obscuros, exigindo que as plataformas adotem uma abordagem mais responsável e transparente em relação ao *design* de suas interfaces e à influência sobre o comportamento dos usuários. Essa exigência representa um avanço na regulação do mercado digital, pois obriga as empresas a considerar ativamente o impacto de suas práticas sobre os consumidores e a tomar medidas para evitar comprometer a autonomia dos usuários.²⁴⁷

²⁴⁵ JABŁONOWSKA, Agnieszka et al. *Exploring the Dark Patterns in Big Data: Big Data and Algorithms in the Digital Marketplace*. European Law Journal, 2018, p. 555.

²⁴⁶ MELO JUNIOR, Glauto Lisboa. *Navegando por padrões obscuros: uma análise crítica da Lei dos Mercados Digitais (DMA) e da Lei dos Serviços Digitais (DSA) para a proteção dos consumidores online*. Revista da Faculdade de Direito da Universidade de Lisboa, Lisboa, v. 64, n. 2, p. 545-573, 2023.

²⁴⁷ MELO JUNIOR, Glauto Lisboa. *Navegando por padrões obscuros: uma análise crítica da Lei dos Mercados Digitais (DMA) e da Lei dos Serviços Digitais (DSA) para a proteção dos consumidores online*. Revista da Faculdade de Direito da Universidade de Lisboa, Lisboa, v. 64, n. 2, p. 545-573, 2023.

Tanto o DMA quanto o DSA têm o potencial de fortalecer a aplicação transfronteiriça e harmonizada das regras de proteção ao consumidor, especialmente em um mercado digital cada vez mais globalizado. No entanto, esse objetivo pode ser parcialmente comprometido pela escolha de focar a regulamentação nos chamados *gatekeepers*, grandes plataformas que atuam como intermediárias entre consumidores e serviços digitais. Embora essa abordagem seja eficaz para controlar as práticas das maiores empresas do setor, ela pode deixar lacunas na proteção dos consumidores que interagem com plataformas menores ou menos reguladas. Isso levanta questões sobre a necessidade de expandir o alcance das regulamentações para garantir que todos os consumidores estejam igualmente protegidos contra práticas desleais e manipulativas.²⁴⁸

É importante destacar que a implementação eficaz dessas regulamentações exigirá um esforço contínuo por parte das autoridades reguladoras, que deverão estar preparadas para identificar, monitorar e combater as práticas de padrões obscuros de maneira proativa. Isso inclui a necessidade de desenvolver ferramentas e métodos mais avançados para detectar essas práticas, além de promover uma maior colaboração entre as autoridades reguladoras dos diferentes países membros da União Europeia para assegurar que as normas sejam aplicadas de maneira uniforme e eficaz em todo o território europeu.²⁴⁹

O DMA e o DSA representam um avanço significativo na proteção dos consumidores no ambiente digital, ao reconhecer a necessidade de uma regulação que vá além das tradicionais medidas antitruste.²⁵⁰ Ao focar nos padrões obscuros, esses regulamentos não só reforçam a proteção dos dados, mas também promovem a equidade e a transparência nos mercados digitais, assegurando que os consumidores tenham controle sobre suas informações e escolhas. O DMA, em particular, pode servir como um modelo regulatório inspirador para outras jurisdições, incluindo o Sistema Brasileiro de Defesa da Concorrência (SBDC), que poderia adotar medidas semelhantes para garantir um mercado digital mais justo e transparente. A

²⁴⁸ GRIMM, Dieter. *L'autorégulation régulée dans la tradition de l'État constitutionnel*. Trivium, Paris, n. 21, 2016.

²⁴⁹ MELO JUNIOR, Glauto Lisboa. *Navegando por padrões obscuros: uma análise crítica da Lei dos Mercados Digitais (DMA) e da Lei dos Serviços Digitais (DSA) para a proteção dos consumidores online*. Revista da Faculdade de Direito da Universidade de Lisboa, Lisboa, v. 64, n. 2, p. 545-573, 2023.

²⁵⁰ SANTOS, Humberto Cunha dos. *Digital Markets Act e suas implicações para a concorrência digital*. JOTA, 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/digital-markets-act-25112022>. Acesso em: 09 set. 2024.

incorporação das práticas regulatórias do DMA pelo SBDC pode resultar em um aprimoramento significativo na proteção de dados e dos direitos dos consumidores no Brasil.²⁵¹

Essas regulamentações europeias, embora sejam pioneiras, integram um movimento global pela proteção dos consumidores no ambiente digital. No entanto, a efetiva implementação dessas normas demanda uma análise mais ampla, levando em consideração os marcos legais existentes, tanto nacionais quanto internacionais, que buscam regular esse mercado em constante evolução. Nesse sentido, é essencial explorar como diferentes jurisdições têm se adaptado para enfrentar os desafios do comércio eletrônico e da proteção ao consumidor no cenário digital, tema que será abordado no próximo tópico sobre os marcos legais de proteção ao consumidor em nível nacional e internacional.

3.3 MARCOS LEGAIS NACIONAIS E INTERNACIONAIS DE PROTEÇÃO AO CONSUMIDOR NO AMBIENTE DIGITAL

A proteção ao consumidor no ambiente digital tem evoluído constantemente em resposta ao crescimento das transações comerciais eletrônicas e à importância cada vez maior dos dados pessoais nas relações econômicas. No contexto internacional, a proteção ao consumidor começou a ser delineada de forma mais estruturada com a publicação das diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em 1980. Essas diretrizes estabeleceram normas mínimas para o tratamento de dados pessoais, buscando garantir a privacidade dos indivíduos e, ao mesmo tempo, assegurar o fluxo livre de informações entre os países.²⁵² Essas diretrizes foram pioneiras na definição de padrões globais para a proteção de dados.

Na sequência, a Convenção 108 do Conselho da Europa, aprovada em 1981, foi a primeira legislação internacional vinculante dedicada à proteção de dados e privacidade no comércio digital. Essa convenção estabeleceu princípios fundamentais sobre a coleta e o processamento de dados pessoais, criando um marco que viria a

²⁵¹ KIRA, Beatriz. *As big techs e a nova onda de regulação digital ao redor do mundo*. JOTA, 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/as-big-techs-e-a-nova-onda-de-regulacao-digital-21072022>. Acesso em: 09 set. 2024.

²⁵² ALMEIDA FILHO, Ednaldo Rodrigues de. *O regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional*. 2020. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2020. p. 65.

influenciar diversas legislações subsequentes, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. A Convenção 108 foi fundamental para moldar o cenário regulatório internacional e estabelecer bases para a proteção dos direitos dos consumidores.²⁵³

O Regulamento Geral de Proteção de Dados (GDPR), que entrou em vigor em 2018, elevou consideravelmente os padrões de proteção de dados na Europa. Esse regulamento impõe obrigações rigorosas às empresas que processam dados de cidadãos europeus, exigindo consentimento explícito para a coleta desses dados e impondo sanções severas para o descumprimento de suas normas.²⁵⁴ O GDPR é hoje uma referência global em termos de proteção de dados e tem impacto direto sobre empresas e legislações de outras nações, como o Brasil.

Além da Europa, outras regiões também têm buscado desenvolver suas próprias regulamentações para lidar com os desafios da era digital. Na Ásia-Pacífico, a Cooperação Econômica Ásia-Pacífico (APEC) implementou o sistema de Regras de Privacidade Transfronteiriças (CBPR), que visa facilitar a transferência de dados entre os países membros, garantindo que as empresas sigam práticas mínimas de proteção de dados em transações internacionais.²⁵⁵ Esse sistema busca promover um ambiente digital seguro e confiável, fundamental para o desenvolvimento sustentável do comércio eletrônico global.

Em paralelo, a Organização Mundial do Comércio (OMC) tem se preocupado em equilibrar as necessidades do comércio internacional com a proteção dos consumidores no ambiente digital. A OMC reconhece que o livre fluxo de dados é essencial para o desenvolvimento econômico global, mas também sublinha que a privacidade e a segurança dos consumidores devem ser priorizadas nas transações digitais.²⁵⁶ A falta de uma regulamentação global uniforme, no entanto, continua sendo um desafio significativo.

No Brasil, a proteção ao consumidor tem uma base sólida no Código de Defesa do Consumidor (CDC), promulgado em 1990. Esse código é amplamente reconhecido

²⁵³ SOARES, Ricardo Maurício Freire. *O princípio constitucional da dignidade da pessoa humana: em busca do direito justo*. São Paulo: Saraiva, 2010. p. 45.

²⁵⁴ LEMOS, Ronaldo. *Proteção de Dados e o Direito à Privacidade*. Rio de Janeiro: Zahar, 2018. p. 32.

²⁵⁵ ALMEIDA FILHO, Ednaldo Rodrigues de. *O regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional*. 2020. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2020. p. 81.

²⁵⁶ SANTOS, Roberta. *A Regulação Internacional do Comércio Digital*. Revista de Direito Internacional, v. 21, n. 1, p. 88-104, 2017. p. 92.

como uma das legislações mais avançadas do mundo no que tange à proteção do consumidor, abordando desde a segurança de produtos e serviços até o direito à informação. O CDC também garante que os consumidores tenham acesso a informações sobre seus dados pessoais armazenados em cadastros e registros, conforme estabelecido no artigo 43.²⁵⁷ O Código Civil de 2002, em seu art. 12, complementa essa proteção ao assegurar o direito à privacidade e à intimidade dos cidadãos.²⁵⁸

O Código de Defesa do Consumidor (CDC) é amplamente reconhecido como uma legislação de vanguarda na proteção dos direitos dos consumidores no Brasil. Sua abrangência e detalhamento estabelecem um marco jurídico que assegura direitos, como a proteção saúde e segurança do consumidor, além de garantir informações claras e precisas sobre produtos e serviços oferecidos no mercado.

No contexto digital, o CDC mantém sua relevância ao estabelecer diretrizes que protegem os consumidores em transações eletrônicas. A exigência de informações claras e precisas sobre produtos e serviços, bem como a garantia de segurança nas operações, são princípios que se aplicam plenamente ao comércio eletrônico. A jurisprudência brasileira tem interpretado o CDC de forma a abranger as novas modalidades de consumo, assegurando que os direitos dos consumidores sejam preservados mesmo diante das inovações tecnológicas.²⁵⁹

No contexto do Código de Defesa do Consumidor (CDC), práticas como as *dark patterns* podem ser interpretadas como formas de "venda casada", que é proibida pelo artigo 39, inciso I, do CDC. Essa proibição visa impedir que fornecedores condicionem a aquisição de um produto ou serviço à compra de outro, protegendo assim a liberdade de escolha do consumidor.²⁶⁰

Quando uma interface digital é projetada de maneira a ocultar opções de recusa ou a induzir a aceitação de produtos ou serviços adicionais, sem o consentimento claro do consumidor, configura-se uma prática abusiva. Essa conduta viola o direito à informação adequada e clara, previsto no artigo 6º, inciso III, do CDC, e pode ser

²⁵⁷ BRASIL. *Lei nº 8.078, de 11 de setembro de 1990*. Código de Defesa do Consumidor. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 10 set. 2024.

²⁵⁸ BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/LEIS//2002/L10406compilada.htm. Acesso em: 10 set. 2024.

²⁵⁹ MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 9. ed. São Paulo: Revista dos Tribunais, 2019. p. 97.

²⁶⁰ MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 9. ed. São Paulo: Revista dos Tribunais, 2019. p. 123.

considerada uma forma de venda casada disfarçada, uma vez que o consumidor é levado a adquirir algo que não desejava originalmente.²⁶¹

As práticas que limitam a liberdade de escolha do consumidor ou que o induzem em erro são contrárias aos princípios do CDC. Sendo assim, a utilização de *dark patterns* que resultem na imposição de produtos ou serviços adicionais pode ser considerada ilegal, sujeitando o fornecedor às sanções previstas no artigo 56 do CDC, que incluem multas, suspensão de atividades e outras medidas administrativas.²⁶²

O Decreto nº 7.962, de 15 de março de 2013, representa um avanço significativo na regulamentação do comércio eletrônico no Brasil, ao estabelecer diretrizes específicas para a proteção do consumidor nesse ambiente. Este decreto complementa o Código de Defesa do Consumidor (CDC) ao detalhar obrigações para fornecedores que atuam no comércio eletrônico, como a disponibilização de informações claras sobre produtos e serviços, a identificação completa do fornecedor e a garantia de um atendimento eficaz ao consumidor.²⁶³

Com a promulgação da Lei Geral de Proteção de Dados (LGPD) em 2018, o cenário jurídico brasileiro passou a contar com uma regulamentação abrangente sobre o tratamento de dados pessoais. A LGPD estabelece princípios e obrigações para o tratamento de dados, visando proteger os direitos fundamentais de liberdade e privacidade dos indivíduos. No contexto do comércio eletrônico, a LGPD reforça as disposições do Decreto nº 7.962/2013, ao exigir que os fornecedores obtenham o consentimento explícito dos consumidores para o tratamento de seus dados pessoais e assegurem a transparência nas operações realizadas.²⁶⁴

Além da LGPD, outras normas contribuem para a proteção do consumidor no ambiente digital. O Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios, garantias e direitos para o uso da internet no Brasil, incluindo a proteção da privacidade e dos dados pessoais dos usuários. A integração dessas normas cria um arcabouço jurídico amplo que busca equilibrar o desenvolvimento do comércio

²⁶¹ MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 9. ed. São Paulo: Revista dos Tribunais, 2019. p. 98.

²⁶² NUNES, Luiz Antonio Rizzatto. *Curso de Direito do Consumidor*. 12. ed. São Paulo: Saraiva, 2018. p. 45.

²⁶³ 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 nov. 2024.

²⁶⁴ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 3. ed. Rio de Janeiro: Renovar, 2021. p. 12.

eletrônico com a proteção dos direitos dos consumidores, promovendo um ambiente digital mais seguro e confiável.²⁶⁵

A harmonização entre o Decreto nº 7.962/2013, a LGPD e outras legislações pertinentes é essencial para assegurar a efetividade da proteção ao consumidor no ambiente digital. Essa integração normativa permite que os consumidores tenham seus direitos resguardados de forma abrangente, desde a transparência nas informações e nas transações comerciais até a segurança e privacidade de seus dados pessoais. Dessa forma, o ordenamento jurídico brasileiro busca acompanhar as evoluções tecnológicas e os desafios impostos pelo comércio eletrônico, garantindo a proteção dos consumidores em todas as suas dimensões.

Fortemente inspirada pelo GDPR, a LGPD trouxe inovações significativas, como a exigência de consentimento explícito para o tratamento de dados pessoais e a criação da Autoridade Nacional de Proteção de Dados (ANPD), responsável por fiscalizar o cumprimento da lei e aplicar sanções em caso de infrações.²⁶⁶ A LGPD visa criar um ambiente de confiança para o comércio eletrônico no Brasil, garantindo que as empresas sejam transparentes no uso dos dados pessoais e assegurando a proteção dos direitos dos consumidores. Entre os principais pilares da LGPD estão a transparência, a responsabilidade das empresas e a proteção da privacidade dos cidadãos, elementos fundamentais para a construção de uma economia digital segura.²⁶⁷

Outro avanço importante na proteção dos consumidores brasileiros no ambiente digital é o Marco Civil da Internet, sancionado pela Lei nº 12.965/2014. Esse marco regula o uso da *internet* no Brasil e estabelece princípios fundamentais como a neutralidade da rede, a privacidade online e a liberdade de expressão. O Marco Civil complementa as disposições do CDC e da LGPD, formando um conjunto de leis que protege os consumidores em suas interações no ambiente digital.²⁶⁸

A criação da Autoridade Nacional de Proteção de Dados (ANPD) foi um passo essencial para garantir o cumprimento da LGPD no Brasil. A ANPD desempenha um

²⁶⁵ BIONI, Bruno Ricardo, *Proteção de Dados Pessoais: a função e os limites do consentimento*, Rio de Janeiro: Forense, 2019. p. 89.

²⁶⁶ BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 set. 2024.

²⁶⁷ COTS, Márcio; OLIVEIRA, Ricardo. *LGPD: Lei Geral de Proteção de Dados comentada*. 3. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 102.

²⁶⁸ BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 set. 2024.

papel de grande relevância ao monitorar o tratamento de dados pessoais no país e assegurar que as empresas estejam em conformidade com a legislação. Além disso, a ANPD, através de seus guias, tem a responsabilidade de conscientizar tanto empresas quanto consumidores sobre a importância da proteção de dados no ambiente digital.²⁶⁹

A cooperação internacional é um elemento-chave para garantir a proteção eficaz dos consumidores no ambiente digital, especialmente em casos que envolvem múltiplas jurisdições. O Acordo de Assistência Mútua (MLAT) facilita a coleta de provas e a condução de investigações transnacionais, sendo uma ferramenta fundamental para combater violações de dados pessoais que atravessam fronteiras.²⁷⁰ A colaboração entre autoridades de diferentes países é essencial para garantir que as legislações nacionais sejam aplicadas de maneira eficaz em um contexto globalizado.

Na América Latina, a Rede Iberoamericana de Proteção de Dados tem desempenhado um papel importante na harmonização das legislações de proteção de dados entre os países da região. Essa rede promove a cooperação jurídica e busca implementar elevados padrões de proteção ao consumidor, especialmente no que tange à privacidade e à segurança dos dados no ambiente digital.²⁷¹ A criação de um ambiente jurídico harmonizado facilita o intercâmbio de informações e o desenvolvimento de estratégias conjuntas para enfrentar os desafios globais relacionados à proteção de dados.

A harmonização regulatória internacional é fundamental para lidar com os desafios impostos pela globalização e pela crescente interconectividade das economias. De acordo com Kuner, a regulação do fluxo de dados entre países deve ser vista como uma forma de pluralismo jurídico, onde diferentes sistemas legais coabitam sem uma hierarquia normativa clara. Isso reflete a realidade da regulação internacional de dados, na qual não há uma norma superior que resolva os conflitos

²⁶⁹ ALMEIDA FILHO, Ednaldo Rodrigues de. *O regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional*. 2020. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2020. p. 95.

²⁷⁰ ABADE, Denise Neves. *Direitos fundamentais na cooperação jurídica internacional*. São Paulo: Saraiva, 2013. p. 110.

²⁷¹ AGUIAR, Thaís. *Cooperação internacional em proteção de dados: conhecendo a Rede Iberoamericana de Proteção de Dados e seu Fórum da Sociedade Civil*. DataPrivacyBR Research, 23 ago. 2022.

de maneira definitiva.²⁷²

Vicente destaca que o objetivo da harmonização jurídica é reduzir as disparidades entre as legislações de diferentes países, promovendo uma equivalência funcional entre suas soluções, sem eliminar a diversidade normativa. Essa abordagem permite que os países mantenham suas especificidades jurídicas enquanto trabalham em direção a uma convergência regulatória que facilite o comércio internacional e a proteção dos consumidores.²⁷³

No entanto, a harmonização jurídica também enfrenta desafios significativos. Kuner adverte que ela não deve ser vista como um objetivo final em si, pois pode ocultar disputas políticas que não foram adequadamente resolvidas.²⁷⁴ Além disso, a harmonização pode resultar em normas excessivamente complexas, que acabam por não refletir adequadamente os interesses que motivaram sua criação.²⁷⁵

Chivot e Castro argumentam que a falta de convergência regulatória não afeta apenas a privacidade dos consumidores, mas também a economia.²⁷⁶ A imposição de normas como o GDPR, por exemplo, tem gerado dificuldades para empresas que operam em diversas jurisdições, o que demonstra a necessidade de uma regulamentação mais coesa e global, especialmente em relação aos fluxos internacionais de dados.²⁷⁷

Os desafios impostos pela ausência de uma regulamentação global uniforme ressaltam a importância da cooperação entre os países. Cory, Atkinson e Castro reforçam a necessidade de uma estrutura regulatória global que permita uma governança eficaz da economia digital.²⁷⁸ Assim como foi necessário criar regras econômicas globais após a Segunda Guerra Mundial, os autores defendem que, hoje, é urgente o estabelecimento de diretrizes internacionais para a gestão de dados, que

²⁷² KUNER, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford: OUP Oxford, 2013. p. 160.

²⁷³ VICENTE, Dário Moura. *Direito Comparado – V. 1: introdução e parte geral*. Coimbra: Almedina, 2008. p. 567.

²⁷⁴ KUNER, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford: OUP Oxford, 2013. p. 165.

²⁷⁵ ALMEIDA FILHO, Ednaldo Rodrigues de. *O regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional*. 2020. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2020. p. 95. p. 104.

²⁷⁶ CHIVOT, Elettra; CASTRO, Daniel. *The GDPR: Europe's new privacy law and transatlantic trade*. Center for Data Innovation, 2019. p. 5.

²⁷⁷ ALMEIDA FILHO, Ednaldo Rodrigues de. *O regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional*. 2020. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2020. p. 95. p. 105.

²⁷⁸ CORY, Nigel; ATKINSON, Robert; CASTRO, Daniel. *Principles and Policies for International Data Flows*. Information Technology and Innovation Foundation, 2019.

se tornaram um dos principais motores da economia mundial.²⁷⁹

A interoperabilidade legal também é um fator fundamental para a harmonização regulatória. Mitchell e Mishra defendem que os Estados membros da Organização Mundial do Comércio (OMC) devem adotar uma estrutura regulatória básica para a proteção dos consumidores online, incluindo a prevenção de práticas fraudulentas. Essa interoperabilidade reduziria as barreiras impostas pelas diferentes legislações de proteção de dados, facilitando o fluxo de informações entre os países.²⁸⁰

Nesse sentido, a convergência regulatória, por meio da harmonização jurídica, oferece uma solução viável para lidar com a proteção e transferência de dados pessoais em um contexto internacional, sobretudo no comércio eletrônico. No entanto, como ressaltam diversos autores, essa harmonização deve respeitar as especificidades de cada sistema jurídico, assegurando que as normas sejam aplicáveis sem comprometer a soberania nacional. O desenvolvimento de um arcabouço regulatório global continua sendo um desafio complexo, mas necessário, no cenário atual da economia digital.²⁸¹

Para que os direitos dos consumidores sejam efetivamente protegidos em nível global, é fundamental que a harmonização regulatória seja acompanhada de mecanismos de fiscalização e cooperação internacional, como o MLAT e a Rede Iberoamericana de Proteção de Dados. Esses mecanismos garantem que as empresas sejam responsabilizadas por violações de dados pessoais, independentemente da jurisdição em que operam, e promovem a criação de um ambiente digital mais seguro e confiável para todos.

Assim, a proteção do consumidor no ambiente digital depende de um equilíbrio entre regulamentações nacionais e internacionais, cooperação entre países e o desenvolvimento contínuo de políticas que acompanhem as inovações tecnológicas. Tanto no Brasil, com o CDC, LGPD e Marco Civil da Internet, quanto no cenário internacional, com o GDPR e os acordos de cooperação jurídica, a convergência regulatória se mostra essencial para garantir que os consumidores estejam protegidos

²⁷⁹ ALMEIDA FILHO, Ednaldo Rodrigues de. *O regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional*. 2020. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2020. p. 95. p. 106.

²⁸⁰ MITCHELL, Andrew D.; MISHRA, Neha. *Regulating cross-border data flows in a data-driven world: how WTO law can contribute*. Journal of International Economic Law, v. 22, n. 1, p. 1-34, 2019. p. 24.

²⁸¹ ALMEIDA FILHO, Ednaldo Rodrigues de. *O regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional*. 2020. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2020. p. 95. p. 109.

em um ambiente digital cada vez mais complexo e interconectado.

Portanto, ao abordar a proteção do consumidor no ambiente digital, é essencial também realizar uma análise comparativa entre a legislação brasileira e o *Digital Markets Act* europeu. Esses dois marcos regulatórios oferecem visões distintas sobre como equilibrar os direitos dos consumidores e a dinâmica do mercado digital, o que será explorado no próximo tópico, com foco nas semelhanças e diferenças entre as abordagens brasileira e europeia para assegurar um ambiente digital mais equilibrado.

3.4 ANÁLISE COMPARATIVA DOS DIREITOS DO CONSUMIDOR: LEGISLAÇÃO BRASILEIRA VERSUS DIGITAL MARKET ACT

A proteção ao consumidor, tanto no Brasil quanto na União Europeia, compartilha um objetivo comum: garantir que os consumidores estejam protegidos contra abusos e distorções do mercado. No entanto, as abordagens adotadas por esses dois sistemas diferem significativamente, com o Brasil seguindo uma linha regulatória mais reativa e individualizada, enquanto o *Digital Markets Act (DMA)* da União Europeia adota uma estrutura proativa e voltada para a regulação de grandes plataformas digitais, conhecidas como *gatekeepers*. Essa diferença central no foco de atuação reflete uma diversidade de tradições jurídicas e de prioridades regulatórias.

No Brasil, a principal norma de proteção ao consumidor é o Código de Defesa do Consumidor (CDC), instituído pela Lei 8.078/90. Essa legislação fundamenta-se no princípio da vulnerabilidade do consumidor, reconhecendo que, em uma relação de consumo, o consumidor está em desvantagem em relação ao fornecedor. O CDC, portanto, impõe uma série de obrigações aos fornecedores, incluindo transparência, boa-fé e a proibição de práticas abusivas. Um dos principais pilares do CDC é a boa-fé objetiva, que exige que as partes ajam de maneira ética e justa durante todas as fases de uma transação.²⁸² Esse princípio é essencial para equilibrar a relação de consumo, protegendo o consumidor de práticas que possam prejudicar suas expectativas legítimas.

Já o DMA, aprovado em 2022, introduz uma abordagem completamente diferente. Ele visa regular as grandes plataformas digitais que atuam como *gatekeepers* no mercado digital. Essas plataformas, como *Google*, *Facebook* e

²⁸² MARQUES, Claudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*. São Paulo: Ed. RT, 2004. p. 162.

Amazon, possuem um poder econômico significativo e desempenham um papel fundamental como intermediárias entre empresas e consumidores. O DMA impõe uma série de obrigações rigorosas para evitar que essas empresas consolidem seu poder de forma anticompetitiva, impondo restrições ao uso de dados e proibindo práticas como a autopreferência, que ocorre quando uma plataforma favorece seus próprios serviços em detrimento de concorrentes.²⁸³

Uma das principais inovações trazidas pelo DMA é a regulação *ex ante*. Enquanto o CDC opera predominantemente de forma reativa, regulando após a ocorrência de abusos, o DMA busca prevenir práticas prejudiciais antes que elas se consolidem no mercado. Isso inclui, por exemplo, a obrigação de interoperabilidade entre serviços de diferentes plataformas, o que facilita a competição e a escolha do consumidor.²⁸⁴ No Brasil, embora o CDC seja eficaz em muitos aspectos, ele ainda carece de uma regulação específica voltada para as peculiaridades do ambiente digital, o que deixa algumas lacunas em termos de proteção.

Outro aspecto que diferencia o DMA da legislação brasileira é o foco na promoção da concorrência como um processo em si. Heike Schweitzer argumenta que o DMA não se limita a proteger os interesses dos consumidores, mas também busca assegurar que a concorrência nos mercados digitais continue sendo justa e aberta. Isso representa um afastamento do modelo tradicional de regulação antitruste, que geralmente se concentra em maximizar o bem-estar do consumidor. No Brasil, a proteção do consumidor é o foco central do CDC, que se preocupa em garantir que este não seja prejudicado por práticas abusivas ou enganosas.²⁸⁵

Apesar dessas diferenças, há também pontos de semelhança entre as duas legislações. Tanto o CDC quanto o DMA têm como objetivo proteger os consumidores contra abusos de poder econômico. No Brasil, o CDC impõe uma série de sanções para práticas abusivas, incluindo multas e até a suspensão das atividades comerciais do fornecedor.²⁸⁶ De forma semelhante, o DMA prevê que a Comissão Europeia possa impor multas significativas às plataformas que não cumprirem suas obrigações,

²⁸³ FERNANDES, Victor Oliveira. *Digital Markets Act (DMA) e o Direito da Concorrência na União Europeia: o futuro finalmente chegou?* Jota, Julho de 2022.

²⁸⁴ FERNANDES, Victor Oliveira. *Digital Markets Act (DMA) e o Direito da Concorrência na União Europeia: o futuro finalmente chegou?* Jota, Julho de 2022.

²⁸⁵ SCHWEITZER, Heike. *The Art to Make Gatekeeper Positions Contestable and the Challenge to Know What is Fair: A Discussion of the Digital Markets Act Proposal*. Zeitschrift für europäisches Privatrecht, v. 3, n. 1, p. 503–544, 2021. p. 509.

²⁸⁶ DIAS, Jean Carlos. *Direito Contratual no Ambiente Virtual*. Curitiba: Juruá, 2006. p. 165.

garantindo assim a eficácia da regulação.²⁸⁷ Esses mecanismos são essenciais para garantir que as empresas cumpram as normas estabelecidas e que os consumidores estejam devidamente protegidos.

No entanto, enquanto o CDC se concentra na relação direta entre consumidor e fornecedor, o DMA adota uma perspectiva mais ampla, considerando a estrutura de mercado e o impacto que as grandes plataformas digitais têm sobre a competitividade e a inovação. Segundo Kerber, o DMA adota um regime rígido de regras justamente para criar um ambiente regulatório mais previsível, embora isso possa restringir a flexibilidade das plataformas para se adaptarem às rápidas mudanças no mercado digital.²⁸⁸ No Brasil, por outro lado, a legislação tende a ser mais flexível, ajustando-se a cada caso individual, mas isso também pode levar a uma falta de previsibilidade para as empresas.

O conceito de *gatekeeper*, central no DMA, não tem equivalente na legislação brasileira. Essas plataformas digitais de grande porte são reguladas de forma específica na União Europeia, com o objetivo de evitar que elas abusem de seu poder de mercado. No Brasil, o Conselho Administrativo de Defesa Econômica (Cade) é o principal órgão responsável por regular questões concorrenciais, mas sua atuação no mercado digital ainda é limitada e ocorre de forma pontual, sem uma regulação *ex ante* que trate das peculiaridades das plataformas digitais.²⁸⁹

Outra diferença fundamental está na forma como cada sistema lida com a concentração econômica. No Brasil, o Cade utiliza o faturamento bruto dos grupos econômicos como principal critério para notificação de atos de concentração. No entanto, isso pode deixar de fora operações importantes no mercado digital, que muitas vezes envolvem grandes volumes de dados e bases de usuários, mas cujo faturamento não atinge o limite estipulado pela legislação brasileira.²⁹⁰ Já o DMA considera a posição dominante das plataformas no mercado como um critério-chave para a intervenção, o que reflete uma adaptação mais adequada à dinâmica da

²⁸⁷ FERNANDES, Victor Oliveira. *Digital Markets Act (DMA) e o Direito da Concorrência na União Europeia: o futuro finalmente chegou?* Jota, Julho de 2022.

²⁸⁸ KERBER, Wolfgang. *Taming tech giants with a per se rules approach?* The Digital Markets Act from the “rules vs. standard” perspective. *Concurrences Law Review*, v. 3, n. 1, p. 28–34, 2021. p. 30.

²⁸⁹ RENZETTI, Bruno. *Digital Markets Act e o controle de estruturas no Brasil*. Conjur, 23 de outubro de 2022. Disponível em: <https://www.conjur.com.br/2022-out-23/bruno-renzetti-digital-markets-act-controle-estruturas/>. Acesso em: 18 set. 2024.

²⁹⁰ RENZETTI, Bruno. *Digital Markets Act e o controle de estruturas no Brasil*. Conjur, 23 de outubro de 2022. Disponível em: <https://www.conjur.com.br/2022-out-23/bruno-renzetti-digital-markets-act-controle-estruturas/>. Acesso em: 18 set. 2024.

economia digital.

A implementação das normas do DMA também levanta questões sobre sua interação com outras disposições legais. Conforme Fernandes (2022, p. 2), há dúvidas sobre como o DMA se relaciona com os artigos 101 e 102 do Tratado de Funcionamento da União Europeia, que regulam o direito da concorrência. Essa sobreposição de normas pode gerar conflitos na aplicação das regras, algo que também ocorre no Brasil, onde a interação entre o CDC e a Lei de Defesa da Concorrência nem sempre é clara, especialmente no contexto digital.²⁹¹

Por outro lado, a legislação brasileira de defesa do consumidor se destaca pela ênfase no princípio da transparência, que obriga os fornecedores a fornecerem informações claras, precisas e completas sobre os produtos e serviços que oferecem. Esse princípio também está presente no DMA, que visa garantir que as plataformas digitais operem de maneira transparente, especialmente no que diz respeito ao uso de dados pessoais e à forma como classificam e apresentam os resultados de busca.²⁹²

Essa abordagem preventiva do DMA, que estabelece regras claras para evitar abusos antes que eles ocorram, é uma diferença marcante em relação ao modelo brasileiro. No Brasil, a legislação ainda opera predominantemente de forma reativa, ou seja, intervém somente após a ocorrência de práticas abusivas ou anticompetitivas. Isso pode dificultar a adaptação do sistema brasileiro às rápidas mudanças do mercado digital, onde os abusos podem ocorrer em uma escala muito maior e de forma muito mais rápida do que nos mercados tradicionais.²⁹³

Dessa forma, enquanto o CDC fornece uma base sólida para a proteção ao consumidor, especialmente no que diz respeito à vulnerabilidade do consumidor e à boa-fé objetiva, o DMA introduz uma série de inovações que podem servir de inspiração para a modernização da legislação brasileira. Isso inclui a imposição de regras específicas para plataformas digitais, a regulação *ex ante* e o conceito de *gatekeeper*, que poderiam ser adaptados às particularidades do mercado brasileiro.

Apesar das críticas quanto à rigidez das disposições do DMA, é inegável que

²⁹¹ FERNANDES, Victor Oliveira. *Digital Markets Act (DMA) e o Direito da Concorrência na União Europeia: o futuro finalmente chegou?* Jota, julho de 2022. p. 2.

²⁹² DIAS, Jean Carlos. *Direito Contratual no Ambiente Virtual*. Curitiba: Juruá, 2006. p. 165.

²⁹³ SANTOS, Humberto Cunha dos. *A discussão de uma possível lei brasileira de regulação dos mercados digitais*: PL 2768/22 atribui à Anatel competências que o Digital Markets Act atribuiu à Comissão Europeia. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/como-a-regulacao-concorrencial-do-digital-markets-act-pode-inspirar-o-sbdc-25112022>. Acesso em: 12 set. 2024.

ele representa um avanço significativo na regulação dos mercados digitais. Sua aplicação, no entanto, dependerá da capacidade das autoridades europeias de equilibrar a necessidade de intervenção com a flexibilidade necessária para se adaptar às constantes transformações do mercado digital.²⁹⁴ No Brasil, a implementação de uma regulação mais moderna e adaptada ao ambiente digital também exigirá uma maior integração entre os diferentes órgãos reguladores e uma maior conscientização sobre a importância de proteger tanto os consumidores quanto a concorrência em um mercado cada vez mais digitalizado.

O DMA e o CDC, apesar de suas diferenças, compartilham o objetivo de proteger o consumidor e promover um ambiente de mercado justo e competitivo. Ambos os sistemas enfrentam desafios significativos para garantir que suas normas sejam eficazes, especialmente no contexto de uma economia digital global em rápida evolução. O futuro da regulação digital no Brasil poderá se beneficiar das lições aprendidas com o DMA, adaptando suas inovações para as necessidades e especificidades do mercado brasileiro.

Ainda assim, como ressalta Santos, a adaptação de modelos regulatórios estrangeiros, como o DMA, ao contexto brasileiro, exigirá uma análise cuidadosa para garantir que as particularidades do mercado e da legislação brasileira sejam respeitadas.²⁹⁵ Ao mesmo tempo, é fundamental que o Brasil continue a aprimorar sua legislação de defesa do consumidor, especialmente no que diz respeito à proteção no ambiente digital, para garantir que os consumidores estejam devidamente protegidos contra os abusos das grandes plataformas e outras formas de poder econômico.

O DMA visa assegurar uma concorrência justa no mercado digital, ao regular as atividades das grandes plataformas, conhecidas como *gatekeepers*. Essas plataformas têm sido identificadas pela Comissão Europeia como essenciais para a estrutura econômica digital da União Europeia, devido ao seu poder de intermediação e a presença estável no mercado, que dificulta a entrada de novos concorrentes e cria

²⁹⁴ KERBER, Wolfgang. *Taming tech giants with a per se rules approach?* The Digital Markets Act from the “rules vs. standard” perspective. *Concurrences Law Review*, v. 3, n. 1, p. 28–34, 2021. p. 30.

²⁹⁵ SANTOS, Humberto Cunha dos. *A discussão de uma possível lei brasileira de regulação dos mercados digitais*: PL 2768/22 atribui à Anatel competências que o Digital Markets Act atribuiu à Comissão Europeia. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/como-a-regulacao-concorrencial-do-digital-markets-act-pode-inspirar-o-sbdc-25112022>. Acesso em: 12 set. 2024.

dependência econômica entre usuários e negócios.²⁹⁶ Ao instituir a interoperabilidade e a transparência como requisitos, o DMA fortalece o ambiente de negócios, promovendo um mercado mais inclusivo e favorecendo o desenvolvimento econômico a longo prazo.

No contexto de proteção ao consumidor, o DMA inova ao estabelecer uma regulamentação *ex ante*, que antecipa problemas de mercado antes que eles ocorram. Diferente do modelo reativo do Código de Defesa do Consumidor brasileiro, o DMA adota uma abordagem preventiva, que pode ser particularmente útil para evitar práticas anticompetitivas e abusos de mercado no ambiente digital. Estudos indicam que a interoperabilidade e a portabilidade de dados, exigidas pelo DMA, são ferramentas valiosas para incentivar a concorrência e permitir que os consumidores troquem de serviços com mais facilidade, reduzindo o risco de monopólio e promovendo o desenvolvimento de novos negócios.²⁹⁷

Para que o Brasil se inspire no DMA e adapte sua legislação, é fundamental considerar o impacto da regulação *ex ante* no desenvolvimento econômico. Como o DMA facilita o crescimento das pequenas e médias empresas e reduz o poder das plataformas dominantes, ele contribui para um ambiente de mercado mais equilibrado e inclusivo. Essa abordagem regulatória ajuda a moldar uma economia digital ampla, permitindo que empresas menores tenham acesso igual ao mercado e possam prosperar sem enfrentar barreiras desleais impostas por grandes conglomerados tecnológicos.

Para concluir, é evidente que a implementação de um modelo regulatório como o Digital Markets Act (DMA) na União Europeia oferece importantes lições para o desenvolvimento econômico e a proteção do consumidor no Brasil. Ao adotar uma abordagem preventiva e de largo alcance, o DMA não apenas combate práticas anticompetitivas, mas também promove um ambiente de mercado mais justo e transparente, que incentiva a inovação e o acesso igualitário a oportunidades econômicas.

A análise comparativa entre o Código de Defesa do Consumidor (CDC) brasileiro e normas internacionais, como o *Digital Markets Act (DMA)* da União

²⁹⁶ ECIPE. The EU Digital Markets Act: *Assessing the Quality of Regulation*. 2023. Disponível em: <https://ecipe.org>. Acesso em: 07 out. 2024.

²⁹⁷ FLETCHER, Amelia et al. *Prohibition of Self-Preferencing and Interoperability in Digital Platforms*. CEPR, 2021.

Europeia, evidencia a necessidade de fortalecer o CDC para enfrentar os desafios do ambiente digital. Enquanto o CDC foca na proteção do consumidor em relações de consumo tradicionais, o DMA adota uma abordagem proativa, regulando preventivamente as grandes plataformas digitais para evitar práticas anticompetitivas e abusos de mercado. Essa diferença de enfoque ressalta a importância de atualizar o CDC para contemplar as especificidades do mercado digital contemporâneo.

Especialistas em direito do consumidor apontam que a legislação brasileira carece de mecanismos específicos para lidar com as peculiaridades das transações *online* e a atuação das plataformas digitais. Marques destaca que o CDC, embora eficaz em muitos aspectos, não aborda de forma abrangente questões como a proteção de dados pessoais, a transparência nos algoritmos de recomendação e a responsabilidade das plataformas por conteúdos de terceiros. Essa lacuna legislativa pode resultar em uma proteção insuficiente para os consumidores no ambiente digital.²⁹⁸

Com base na principiologia e na teleologia do Código de Defesa do Consumidor, que visam proteger o consumidor de maneira favorável e justa, especialmente aquele que se encontra em posição de vulnerabilidade, é possível observar a ampliação dessa proteção no contexto do ambiente eletrônico. A legislação existente já fornece fundamentos para tratar a vulnerabilidade agravada que o consumidor enfrenta no ambiente digital, onde algoritmos e sistemas de Machine Learning desempenham papel central nas relações de consumo.

Contudo, é necessário dirigir a análise para os vieses e preconceitos que muitas vezes são incorporados aos algoritmos. Estes sistemas de aprendizado de máquina (*Machine Learning*), ao serem treinados com bases de dados extensas (*Big Data*) que podem conter vieses estruturais e culturais, acabam reproduzindo e amplificando esses preconceitos. Como resultado, as novas tecnologias aplicam uma lógica binária, inflexível e incapaz de distinguir nuances em contextos complexos, o que leva a exclusões e discriminações. O programador, ao estabelecer a arquitetura e o funcionamento desses algoritmos, inadvertidamente reforça uma lógica que perpetua injustiças sociais, pois as decisões algorítmicas passam a refletir uma visão simplificada e polarizada do mundo – uma visão que, ao não distinguir zonas

²⁹⁸ MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 9. ed. São Paulo: Revista dos Tribunais, 2019. p. 110.

cinzentas, muitas vezes marginaliza indivíduos e grupos já vulneráveis.²⁹⁹

Nesse sentido, torna-se imperativo que as políticas de proteção ao consumidor e a legislação que regulamenta o uso de algoritmos e tecnologias de inteligência artificial estejam atentas a esses riscos, buscando assegurar que as ferramentas tecnológicas respeitem os princípios de justiça e igualdade, promovendo um ambiente de consumo mais inclusivo e ético.

A experiência europeia com o DMA oferece *insights* valiosos para o aprimoramento do CDC. O DMA estabelece obrigações claras para os chamados *gatekeepers*, incluindo a proibição de práticas como a autopreferência e a exigência de interoperabilidade entre serviços. Essas medidas visam promover a concorrência e proteger os consumidores de abusos de poder econômico. Conforme observa Kerber, a adoção de uma regulação *ex ante*, como a do DMA, pode ser uma estratégia eficaz para prevenir práticas prejudiciais antes que elas se consolidem no mercado.³⁰⁰

Assim, é imperativo que o Brasil considere a modernização do CDC, incorporando princípios e diretrizes que reflitam as realidades do mercado digital. Isso inclui a implementação de medidas preventivas contra práticas abusivas, a garantia de transparência nas operações das plataformas digitais e a proteção efetiva dos dados pessoais dos consumidores. Ao alinhar-se às melhores práticas internacionais, o Brasil poderá assegurar uma proteção mais robusta aos consumidores e fomentar um ambiente de mercado mais justo e competitivo.

No Brasil, a discussão sobre a regulação de plataformas digitais tem avançado por meio de diversos projetos de lei que buscam adaptar a legislação nacional às especificidades do ambiente digital. Um exemplo inicial é o Projeto de Lei nº 3.514/2015, originado como PLS 281/2012 no Senado Federal, propõe significativas atualizações ao Código de Defesa do Consumidor (CDC) para adequá-lo às realidades do comércio eletrônico. Dentre as inovações, destaca-se a inclusão do artigo 3º-A, que determina que as normas e os negócios jurídicos devem ser interpretados e integrados de maneira mais favorável ao consumidor, reforçando a proteção dos seus direitos. Além disso, o projeto enfatiza a relação entre meio ambiente e consumo sustentável, incorporando princípios que promovem práticas de

²⁹⁹ SILVA, Tarcízio. *Racismo algorítmico: inteligência artificial e discriminação nas redes digitais*. Edições Sesc SP, 2022. p. 72.

³⁰⁰ KERBER, Wolfgang. *Taming Tech Giants with a Per-Se Rules Approach? The Digital Markets Act from the 'Rules vs. Standards' Perspective*. *Concurrences Review*, n. 3, p. 256, 2021. p. 2.

produção e consumo responsáveis. No que tange à privacidade e segurança, os incisos XI e XII do artigo 6º abordam a proteção das informações e dados pessoais em qualquer ambiente, inclusive o eletrônico, e asseguram a liberdade de escolha frente a novas tecnologias e redes de dados, vedando qualquer forma de discriminação e assédio de consumo.³⁰¹

O PL 3.514/2015 também reforça o dever de informar e de cooperar nos ambientes digitais. Propõe dispositivos específicos que objetivam o fortalecimento da confiança e a tutela da expectativa do consumidor, como o artigo 45-A, que estabelece uma série de informações que devem estar presentes na oferta ou conclusão dos contratos. Essas medidas visam garantir maior transparência nas transações online e assegurar que os consumidores estejam plenamente informados sobre os produtos e serviços adquiridos, promovendo um ambiente de consumo mais seguro e confiável.³⁰²

Outro exemplo inicial é o Projeto de Lei nº 2.630/2020, conhecido como "PL das Fake News", que propõe a criação da Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Esse projeto busca combater a disseminação de notícias falsas e conteúdos prejudiciais nas redes sociais e aplicativos de mensagens, estabelecendo obrigações para as plataformas digitais em relação à identificação de usuários e à moderação de conteúdo. A proposta tem gerado debates intensos sobre a necessidade de equilibrar a liberdade de expressão com a responsabilidade no ambiente digital.³⁰³

Posteriormente, o Projeto de Lei nº 2.768/2022, apresentado pelo deputado João Maia (PL/RN), propõe atribuir à Agência Nacional de Telecomunicações (Anatel) a responsabilidade de regular o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro. A iniciativa visa estabelecer diretrizes claras para a atuação dessas plataformas, garantindo maior transparência e responsabilidade em suas operações. Além disso, o projeto prevê a criação de uma

³⁰¹ BRASIL. Congresso Nacional. *Projeto de Lei nº 3.514, de 2015*. Altera a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre o comércio eletrônico e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2052488>. Acesso em: 19 nov. 2024.

³⁰² BRASIL. Congresso Nacional. *Projeto de Lei nº 3.514, de 2015*. Altera a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre o comércio eletrônico e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2052488>. Acesso em: 19 nov. 2024.

³⁰³ BRASIL. Senado Federal. *Projeto de Lei nº 2.630, de 2020*. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>. Acesso em: 19 nov. 2024.

taxa de fiscalização a ser paga pelas grandes empresas do setor, com o objetivo de financiar as atividades de supervisão e assegurar o cumprimento das normas estabelecidas.³⁰⁴

O Projeto de Lei nº 2.338, de 2023, apresentado pelo senador Rodrigo Pacheco, estabelece normas gerais para o desenvolvimento, implementação e uso responsável de sistemas de Inteligência Artificial (IA) no Brasil. O PL visa proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico. Entre suas diretrizes, destacam-se a transparência, a explicabilidade e a auditabilidade dos sistemas de IA, além da promoção de inovação responsável e da proteção de dados pessoais. O projeto encontra-se em tramitação no Senado Federal, sob a relatoria do senador Eduardo Gomes, e tem sido objeto de análises e contribuições de diversas entidades, incluindo a Autoridade Nacional de Proteção de Dados (ANPD).³⁰⁵

Por fim, destaca-se o Projeto de Lei nº 3.024/2024, de autoria do senador Jader Barbalho (MDB/PA), que propõe responsabilizar solidariamente as plataformas de comércio eletrônico pela venda direta ou indireta de produtos falsificados. Essa iniciativa visa fortalecer a proteção ao consumidor no ambiente digital, assegurando que as plataformas adotem medidas eficazes para prevenir a comercialização de mercadorias ilegais. O projeto determina que as plataformas implementem políticas internas de prevenção, incluindo a remoção de ofertas ilegais e a suspensão de vendedores infratores, além de realizar auditorias periódicas para assegurar o cumprimento das políticas de uso e da legislação aplicável. Atualmente, o PL 3.024/2024 encontra-se em tramitação no Senado Federal, aguardando parecer na Comissão de Comunicação e Direito Digital.³⁰⁶

Esses projetos de lei evidenciam o esforço do legislativo brasileiro em acompanhar as transformações do mercado digital e em garantir a proteção dos

³⁰⁴ BRASIL. Câmara dos Deputados. *Projeto de Lei nº 2.768, de 2022*. Dispõe sobre a organização, o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro e dá outras providências. Brasília, DF: Câmara dos Deputados, 2022. Disponível em: <https://www.camara.leg.br/propostas-legislativas/2337417>. Acesso em: 19 nov. 2024.

³⁰⁵ BRASIL. Senado Federal. *Projeto de Lei nº 2.338, de 2023*. Estabelece normas gerais para o desenvolvimento e uso de sistemas de Inteligência Artificial. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 19 nov. 2024.

³⁰⁶ BRASIL. Senado Federal. *Projeto de Lei nº 3.024, de 2024*. Dispõe sobre a responsabilidade solidária das plataformas de comércio eletrônico pela venda de produtos falsificados. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/156789>. Acesso em: 19 nov. 2024.

consumidores e a concorrência justa. A adoção de medidas inspiradas em legislações internacionais, como o *Digital Markets Act* da União Europeia, pode contribuir para o desenvolvimento de um marco regulatório mais eficaz e adaptado às particularidades do ambiente digital brasileiro. No entanto, é fundamental que essas iniciativas considerem as especificidades do contexto nacional e promovam um equilíbrio adequado entre inovação, liberdade de expressão e responsabilidade no uso das plataformas digitais.

Ante ao exposto, os sistemas jurídicos brasileiro e europeu, embora convergentes na finalidade de proteger o consumidor e promover a concorrência, foram concebidos sob bases históricas e prioridades normativas diversas. No Brasil, a legislação consumerista está ancorada principalmente no Código de Defesa do Consumidor (Lei 8.078/90), reforçado por projetos de lei em tramitação que buscam sua modernização para o ambiente digital, já no contexto europeu, o ordenamento jurídico adota uma estrutura mais abrangente e preventiva, materializada em normativas como o *Digital Markets Act (DMA)*, voltadas ao combate de abusos estruturais em plataformas digitais de grande porte.

A distinção entre esses modelos pode ser explicada pela forma como cada um deles foi concebido, pois o CDC foi criado em uma época em que o comércio digital ainda não figurava como elemento central da economia, resultando em uma lei que, à época, se mostrava suficiente para proteger o consumidor em relações de consumo tradicionais. No entanto, o acelerado desenvolvimento tecnológico e a expansão do comércio virtual trouxeram novas demandas, sendo abordadas de maneira pontual por projetos de lei que visam, entre outros aspectos, regular práticas enganosas conhecidas no ambiente digital. O DMA, por outro lado, já surge em um mercado digital consolidado, focando-se em inibir preventivamente condutas nocivas por parte de plataformas capazes de influenciar grandes segmentos econômicos.

No ordenamento brasileiro, a ausência de dispositivos específicos o tema tem levado à discussão sobre um aprimoramento normativo que contemple os desafios da economia digital. Diversas proposições legislativas, como as demonstradas, discutem a responsabilidade de plataformas em relação à transparência, governança de dados e contenção de práticas abusivas. Essa construção gradativa busca harmonizar princípios tradicionais do CDC, como a boa-fé objetiva e a vulnerabilidade do consumidor, com as realidades de um mercado digital em constante evolução.

No âmbito europeu, além do DMA, outras normativas complementares atuam

na conformação de um mercado único digital, reforçando a proteção do consumidor e a defesa da concorrência. Diferentemente do modelo brasileiro, que historicamente adota uma postura predominantemente reativa, o arcabouço europeu prioriza a regulação *ex ante* de plataformas digitais, estabelecendo regras claras sobre interoperabilidade, limitações ao uso de dados e proibições de práticas que induzam o usuário a comportamentos contrários ao seu interesse. Essa estratégia busca garantir a livre concorrência e impedir a formação de posições de domínio difíceis de reverter posteriormente.

Ao observar os sistemas jurídico-normativos brasileiro e europeu, fica evidente que ambos têm objetivos convergentes, porém seguem metodologias distintas, enquanto o Brasil está em fase de elaboração de normas específicas para acompanhar a crescente complexidade do mercado digital, a União Europeia conta com uma estrutura já consolidada, aplicando regulações voltadas diretamente a plataformas gigantes e seus impactos econômicos e sociais. A experiência europeia, materializada no DMA, oferece importantes reflexões para o ordenamento brasileiro, que encontra no aprimoramento legislativo — por meio de projetos de lei e do próprio aperfeiçoamento do CDC — uma via para estabelecer um sistema normativo capaz de equilibrar inovação tecnológica e efetiva proteção aos consumidores.

No que tange à responsabilização civil das plataformas digitais no contexto brasileiro, isso é uma questão que tem sido amplamente debatida, especialmente no Superior Tribunal de Justiça (STJ). No *Recurso Especial nº 1.836.349-SP*, o STJ analisou a responsabilidade de plataformas *marketplace* em situações onde sua atuação contribui para a ocorrência de danos ao consumidor.³⁰⁷ Nesse julgamento, o tribunal reconheceu que a plataforma pode ser incluída na cadeia de fornecimento, dependendo do nível de intervenção e controle que exerce sobre a relação de consumo. Esse entendimento está fundamentado nos artigos 3º e 7º, parágrafo único, do Código de Defesa do Consumidor (CDC), que preveem a responsabilidade solidária dos fornecedores nas relações de consumo.³⁰⁸

³⁰⁷ BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.836.349-SP*. Relator: Min. Ricardo Villas Bôas Cueva. Brasília, 27 ago. 2019. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=2181939&tipo=0&nreg=201901346226&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20220624&formato=HTML&salvar=false>. Acesso em: 18 set. 2024.

³⁰⁸ MUCELIN, Guilherme; JABRA, Alexandre. *Responsabilização de plataformas segundo STJ: aplicação-fornecedora*. Consultor Jurídico, 4 out. 2023. Disponível em: <https://www.conjur.com.br/2023-out-04/garantias-consumo-responsabilizacao-plataformas-segundo-stj2/>. Acesso em: 18 set. 2024.

O STJ diferencia a atuação das plataformas entre facilitadoras e intermediadoras, enquanto as facilitadoras atuam como meros anunciantes, sem intermediar diretamente as transações, as intermediadoras exercem controle significativo, oferecendo serviços como cobrança de pagamento, garantias, avaliações e suporte ao consumidor. Quando a plataforma adota uma postura de controle ou intervenção, extrapolando o papel de simples meio de divulgação, ela passa a integrar a cadeia de fornecimento e, portanto, responde solidariamente pelos danos causados ao consumidor. Essa distinção é fundamental para determinar a responsabilidade objetiva da plataforma, conforme estabelecido no CDC.³⁰⁹

A teoria do risco, consagrada no artigo 927, parágrafo único, do Código Civil, fundamenta a responsabilidade objetiva das plataformas intermediadoras. Ao explorarem a atividade econômica no ambiente digital, elas assumem os riscos inerentes, sendo responsáveis por reparar os danos sofridos pelos consumidores, independentemente de culpa. Nesse sentido, o STJ, ao decidir o caso mencionado, reafirma que a vulnerabilidade do consumidor deve prevalecer como critério central na interpretação das relações digitais, garantindo sua proteção constitucional nos termos do artigo 5º, XXXII, da Constituição Federal.³¹⁰

No cenário das plataformas *marketplace*, a confiança dos consumidores é um ativo essencial, e sua manutenção depende de garantias oferecidas pelas plataformas quanto à segurança e à transparência das transações. O STJ, ao exigir uma análise contextualizada de cada caso, reconhece que a plataforma pode ser responsabilizada se sua atuação contribuir para a concretização de danos. Assim, plataformas que facilitam fraudes, seja por falhas nos mecanismos de verificação ou pela omissão na garantia de segurança das transações, devem responder objetivamente pelos prejuízos sofridos pelos consumidores, como ocorreu no *REsp nº 1.836.349-SP*.³¹¹

Por fim, a decisão do STJ reflete a necessidade de adaptar a aplicação das normas do CDC à realidade das plataformas digitais, considerando a complexidade e

³⁰⁹ MUCELIN, Guilherme; JABRA, Alexandre. *Responsabilização de plataformas segundo STJ: aplicação-fornecedora*. Consultor Jurídico, 4 out. 2023. Disponível em: <https://www.conjur.com.br/2023-out-04/garantias-consumo-responsabilizacao-plataformas-segundo-stj2/>. Acesso em: 18 set. 2024.

³¹⁰ MUCELIN, Guilherme; JABRA, Alexandre. *Responsabilização de plataformas segundo STJ: aplicação-fornecedora*. Consultor Jurídico, 4 out. 2023. Disponível em: <https://www.conjur.com.br/2023-out-04/garantias-consumo-responsabilizacao-plataformas-segundo-stj2/>. Acesso em: 18 set. 2024.

³¹¹ BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.836.349-SP*. Relator: Min. Ricardo Villas Bôas Cueva. Brasília, 27 ago. 2019. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=2181939&tipo=0&nreg=201901346226&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20220624&formato=HTML&salvar=false>. Acesso em: 18 set. 2024.

a multimodalidade dos arranjos comerciais contemporâneos. A responsabilidade civil dessas plataformas deve ser analisada caso a caso, levando em conta o nível de controle e ingerência na relação de consumo. Esse entendimento protege os consumidores no ambiente digital e promove o equilíbrio entre as partes envolvidas, alinhando-se aos princípios fundamentais do direito do consumidor brasileiro.

CONSIDERAÇÕES FINAIS

A presente dissertação evidenciou que a digitalização das relações de consumo e o crescimento do comércio eletrônico trouxeram significativos desafios à proteção dos consumidores. No ambiente digital, a autonomia dos consumidores é comprometida pelas práticas manipulativas, como os *dark patterns*, que são desenhadas para explorar vulnerabilidades cognitivas. Ao explorar essas práticas, o estudo reforça a urgência de uma regulamentação que promova a transparência e o respeito aos direitos fundamentais, alinhando-se aos princípios da ordem econômica constitucional.

O uso de *dark patterns* em plataformas de *e-commerce* representa uma violação da autodeterminação informativa dos consumidores. Essas práticas comprometem a liberdade de escolha, pois influenciam as decisões de compra de forma velada. A pesquisa identificou que os consumidores muitas vezes são conduzidos a ações que favorecem interesses empresariais, em detrimento de seus próprios direitos, evidenciando uma lacuna na legislação brasileira para proteger adequadamente os consumidores no ambiente digital.

Ao abordar o contexto do comércio eletrônico, o estudo constatou que os princípios constitucionais de dignidade e proteção do consumidor são desafiados pela manipulação algorítmica. A pesquisa comparativa com o modelo europeu, onde o *Digital Markets Act* e o *Digital Services Act* estabelecem uma abordagem *ex ante* para evitar abusos de mercado, sugere que o Brasil pode aprender com essas experiências e buscar uma regulação que também antecipe problemas, garantindo um equilíbrio entre inovação e segurança. Além disso, a pesquisa revelou que a vulnerabilidade digital é acentuada para consumidores com menor conhecimento tecnológico. Assim, para garantir que o princípio da igualdade no consumo seja respeitado, a legislação deve incluir medidas de proteção que assegurem uma participação equitativa no mercado digital para todos.

No contexto da linha de pesquisa "Desenvolvimento Econômico e Princípios Constitucionais da Ordem Econômica," o estudo sublinha a importância de regular o ambiente digital de maneira a promover uma economia inclusiva e justa. A regulamentação que proteja o consumidor contra *dark patterns* não só contribui para a defesa dos direitos fundamentais, mas também fortalece a ordem econômica ao garantir que os mercados operem de forma transparente e responsável.

A pesquisa aponta que a manipulação algorítmica, ao capturar e utilizar dados pessoais de forma opaca, subverte o princípio de autodeterminação informativa. Essa prática limita a liberdade dos consumidores e demonstra uma assimetria de poder que contraria os ideais de justiça e igualdade. O estudo destaca que a implementação de normas de transparência na coleta e uso de dados é essencial para garantir que o direito à privacidade seja respeitado.

A análise da legislação brasileira, principalmente o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados, revela que, embora existam disposições gerais para a proteção dos consumidores, essas normas não são suficientemente específicas para lidar com as práticas digitais emergentes. A pesquisa sugere que a adaptação dessas leis, com enfoque na manipulação algorítmica e nos *dark patterns*, é fundamental para assegurar a eficácia das proteções no ambiente digital.

A comparação com as práticas regulatórias da União Europeia revela que uma abordagem preventiva pode ser benéfica para a economia digital brasileira. O *Digital Markets Act*, por exemplo, impõe responsabilidades claras às plataformas digitais, promovendo uma concorrência justa e reduzindo o poder das grandes corporações sobre o consumidor. Adotar diretrizes semelhantes pode fortalecer a economia digital no Brasil, alinhando-se aos princípios constitucionais da ordem econômica.

A proteção contra práticas abusivas, como os *dark patterns*, fortalece a confiança do consumidor no mercado digital. Essa confiança é essencial para o desenvolvimento econômico sustentável, pois um ambiente de consumo justo e transparente incentiva a participação e o crescimento do mercado. O estudo reforça que a proteção ao consumidor deve ser vista como um pilar fundamental para o desenvolvimento econômico no contexto digital.

A análise revelou que a manipulação algorítmica muitas vezes é difícil de detectar, pois atua de forma sutil e oculta. No entanto, seus efeitos são profundos, afetando a privacidade, a liberdade de escolha e, conseqüentemente, a dignidade dos consumidores. Proteger esses direitos é necessário para assegurar que o ambiente digital respeite os valores constitucionais da ordem econômica, que incluem a promoção de uma economia equilibrada e a defesa dos mais vulneráveis.

A pesquisa conclui que uma regulamentação mais rígida e específica é necessária para enfrentar os desafios impostos pelo comércio eletrônico. O ambiente digital exige uma abordagem legal que aborde diretamente as práticas manipulativas

e que promova a transparência. Esse enfoque contribui para a proteção dos direitos do consumidor e para a integridade do mercado, ambos fundamentais para o desenvolvimento econômico.

A proteção ao consumidor digital também deve envolver a colaboração internacional. Como demonstrado na comparação com a União Europeia, a regulamentação *ex ante* permite que os países enfrentem práticas desleais de maneira preventiva. O Brasil, ao buscar parcerias e alinhar-se a essas diretrizes, pode criar uma estrutura regulatória que incentive a inovação ao mesmo tempo que respeita os direitos fundamentais. Nesse contexto, a legislação deve promover a ética, a transparência e a responsabilidade no *design* de interfaces e no uso de algoritmos. Ao fazer isso, o Brasil avança em direção a uma economia digital que respeite a dignidade do consumidor e fortaleça os princípios constitucionais da ordem econômica.

Nesse sentido, embora a regulamentação específica para combater práticas manipulativas, como os *dark patterns*, seja essencial, a simples previsão legal não é suficiente para enfrentar problemas tão profundamente enraizados na sociedade da informação. O dinamismo e a complexidade do ambiente digital demandam uma resposta que vai além da criação de normas, exigindo uma interpretação principiológica que garanta a efetiva proteção do consumidor. Os princípios já consagrados no ordenamento jurídico brasileiro, como a boa-fé objetiva, a transparência e a vulnerabilidade do consumidor, devem ser aplicados de forma ampla e adaptativa para abranger as novas formas de manipulação digital, conferindo maior segurança e equidade nas relações de consumo.

Nesse sentido, o papel do Judiciário torna-se ainda mais relevante diante das limitações do processo legislativo em acompanhar a rápida evolução tecnológica, a jurisprudência tem se mostrado uma ferramenta eficaz para enfrentar essas questões, utilizando os princípios norteadores do Código de Defesa do Consumidor (CDC) e da Constituição Federal para reinterpretar situações inéditas no contexto digital. Decisões como a proferida pelo Superior Tribunal de Justiça (STJ) no Recurso Especial nº 1.836.349-SP, que reconhecem a responsabilidade objetiva das plataformas digitais quando participam da cadeia de consumo, demonstram que a interpretação judicial pode oferecer soluções mais concretas e ajustadas à realidade tecnológica, garantindo proteção aos consumidores mesmo na ausência de normas específicas.

Portanto, mais do que legislações específicas, o que se mostra fundamental é uma atuação coordenada entre os poderes Legislativo e Judiciário, onde a regulação *ex ante* e o fortalecimento das normas existentes caminhem lado a lado com uma interpretação jurídica alinhada aos valores constitucionais. O princípio da dignidade da pessoa humana e a justiça social devem ser os eixos que norteiam a aplicação das normas de proteção ao consumidor no ambiente digital. Somente assim será possível enfrentar os desafios da sociedade da informação, promovendo um mercado mais justo, transparente e ético, que respeite os direitos fundamentais e a autonomia dos consumidores.

REFERÊNCIAS

- ABADE, Denise Neves. **Direitos fundamentais na cooperação jurídica internacional**. São Paulo: Saraiva, 2013.
- AGUIAR, Thaís. **Cooperação internacional em proteção de dados**: conhecendo a Rede Iberoamericana de Proteção de Dados e seu Fórum da Sociedade Civil. DataPrivacyBR Research, 23 ago. 2022.
- AKERLOF, George A.; SHILLER, Robert J. **Pescando tolos**: a economia da manipulação e fraude. Rio de Janeiro: Alta Books, 2016.
- ALMEIDA FILHO, Ednaldo Rodrigues de. **O regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional**. 2020. Dissertação (Mestrado) – Universidade Federal de Pernambuco, Recife, 2020.
- AZEVEDO, Júlio Camargo de. **Delimitando o conceito de vulnerabilidade digital** – Parte I. JOTA.info, 2021. Disponível em: <https://www.jota.info>. Acesso em: 03 set. 2024.
- BAGGIO, Andreza Cristina. **O direito do consumidor brasileiro e a teoria da confiança**. São Paulo: Editora Revista dos Tribunais, 2012.
- BAKOS, Yannis. **Reducing buyer search costs**: implications for electronic marketplaces. Management Science, v. 43, n. 12, 1997.
- BAKSHY, Eytan; MESSING, Solomon; ADAMIC, Lada A. **Exposure to ideologically diverse news and opinion on Facebook**. Science, v. 348, n. 6239, p. 1130-1132, 2015.
- BALDWIN, Robert; CAVE, Martin. **Understanding regulation**: theory, strategy, and practice. Oxford: Oxford University Press, 2011.
- BATOCCHIO, Amália. **Guia nº 3/2022 da EDPB e a discussão sobre dark patterns**. Consultor Jurídico, 5 jul. 2022. Disponível em: <https://www.conjur.com.br/2022-jul-05/direito-digital-guia-32022-edpb-discussao-dark-patterns>. Acesso em: 10 ago. 2024.
- BARRAL, Welber. **Metodologia da pesquisa jurídica**. Editora del Rey, 2007.
- BELL, Daniel. **O advento da sociedade industrial**: uma tentativa de previsão social. São Paulo: Cultrix, 1978.
- BENJAMIN, Antônio Herman de Vasconcellos e. Curso de direito do consumidor. São Paulo: **Revista dos Tribunais**, 2007.
- BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.
- BITTAR, Eduardo CB. **Metodologia da pesquisa jurídica**. Saraiva Educação SA,

2016.

BONILLA, Maria Helena. **Inclusão digital**: polêmica contemporânea. In: PRETTO, Nelson de Luca; BONILLA, Maria Helena (Orgs.). *Inclusão digital: polêmica contemporânea*. Salvador: Edufba, 2005.

BÖSCH, Christoph et al. **Tales from the dark side**: Privacy dark strategies and privacy dark patterns. In: *Proceedings on Privacy Enhancing Technologies*, 2016, n. 4, p. 237-254. Disponível em: <https://doi.org/10.1515/popets-2016-0038>. Acesso em: 09 ago. 2024.

BJORLO, L.; MOEN, O; PASQUINE, M. **The role of consumer autonomy in developing sustainable AI**: A conceptual framework. *Sustainability (Switzerland)*, v. 13, n. 4, p. 1-18, 2021. DOI: 10.3390/su13042332. Acesso em: 11 ago. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 09 ago. 2024.

BRASIL. **Lei n.º 10.406/02 de 10 de janeiro de 2002**. Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 30 jun. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 set. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 07 jul. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 30 jun. 2024.

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 nov. 2024.

BRASIL. Congresso Nacional. **Projeto de Lei nº 3.514, de 2015**. Altera a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre o comércio eletrônico e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=205248>. Acesso em: 19 nov. 2024.

BRASIL. Senado Federal. **Projeto de Lei nº 2.630, de 2020**. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>. Acesso em: 19 nov. 2024.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.768, de 2022**. Atribui à Agência Nacional de Telecomunicações (Anatel) a responsabilidade de regular o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2337417>. Acesso em: 19 nov. 2024.

BRASIL. Senado Federal. **Projeto de Lei nº 2.338, de 2023**. Estabelece normas gerais para o desenvolvimento e uso de sistemas de Inteligência Artificial. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 19 nov. 2024.

BRASIL. Senado Federal. **Projeto de Lei nº 3.024, de 2024**. Dispõe sobre a responsabilidade solidária das plataformas de comércio eletrônico pela venda de produtos falsificados. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/156789>. Acesso em: 19 nov. 2024.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.836.349-SP**. Relator: Min. Ricardo Villas Bôas Cueva. Brasília, 27 ago. 2019. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ITA?seq=2181939&tipo=0&nreg=201901346226&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20220624&formato=HTML&salvar=false>. Acesso em: 18 set. 2024.

BRETON, Philippe. **A manipulação da palavra**. São Paulo: Loyola, 1999.

BRIGNULL, Harry et al. **Deceptive Patterns**: User Interfaces Designed to Trick You. Deceptive.design, 25 abr. 2023. Disponível em: <https://www.deceptive.design>. Acesso em: 05 ago. 2024.

BRIGNULL, Harry. **Dark Patterns**. 2010. Disponível em: <https://darkpatterns.org>. Acesso em: 12 ago. 2024.

BRIGNULL, Harry. **Dark patterns**: Deception vs. honesty in UI design. A List Apart, Issue nº 338, 01 nov. 2011. Disponível em: <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/>. Acesso em: 07 ago. 2024.

BURI, Ilaria; VAN HOBOKEN, Joris. **The Digital Services Act (DSA) proposal**: a critical overview. Digital Services Act (DSA) Observatory Institute for Information Law (IViR), Universidade de Amsterdã, 2021.

CABRAL, Anna Cecília Moreira. Digital Markets Act: porque uma regulação ex ante para plataformas? **Revista de Direito, Inovação, Propriedade Intelectual e Concorrência**, v. 9, n. 1, p. 76–96, jan./jul. 2023.

CANETRO GAMITO, M. Do too many cooks spoil the broth? How EU law underenforcement allows TikTok's violations of minors' rights. **Journal of Consumer Policy**, v. 46, p. 281-305, 2023.

CARDOSO, Simone; KAWAMOTO, Márcia Hiroko; MASSUDA, Ely Mitie. Comércio

eletrônico: o varejo virtual brasileiro. **Revista Cesumar–Ciências Humanas e Sociais Aplicadas**, v. 24, n. 1, p. 117-134, 2019.

CASTELLS, M. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. **A sociedade em rede**: do conhecimento à política. In: CASTELLS, Manuel (Org.); CARDOSO, Gustavo (Org.). *Sociedade em Rede: Do conhecimento à acção política*. Lisboa: Imprensa Nacional, 2005.

CATANI, Afrânio Mendes. **O que é capitalismo**. São Paulo: Editora Brasiliense, 2011.
CHAISSÉ, Valéria Falcão. *A publicidade em face do Código de Defesa do Consumidor*. São Paulo: Saraiva, 2001.

CHIVOT, Elettra; CASTRO, Daniel. **The GDPR**: Europe's new privacy law and transatlantic trade. Center for Data Innovation, 2019.

CLARO, Alberto Carvalho dos Santos. **Comércio Eletrônico**. 1ª Edição: São Paulo, 2013.

COLOMBO, Cristiano; GOULART, Guilherme D. **Hipervulnerabilidade do consumidor no ciberespaço e o tratamento dos dados pessoais à luz da Lei Geral de Proteção de Dados Pessoais Brasileira (LGPD)**. In: 9º Congresso Iberoamericano de Investigadores y Docentes de Derecho e Informática, 2019. Montevideo. Artigo. Disponível em: <http://direitodatecnologia.com/index.php/artigos/>. Acesso em: 06 ago. 2024.

COMPARATO, F. K. **A proteção ao consumidor na Constituição Brasileira de 1988**. *Revista de Direito Mercantil*, n. 80, 1990.

CORY, Nigel; ATKINSON, Robert; CASTRO, Daniel. **Principles and Policies for International Data Flows**. Information Technology and Innovation Foundation, 2019.

COTS, Márcio; OLIVEIRA, Ricardo de (Coord.). **O legítimo interesse e a LGPD**. São Paulo: Revista dos Tribunais, 2020.

COTS, Márcio; OLIVEIRA, Ricardo. **LGPD**: Lei Geral de Proteção de Dados comentada. 3. ed. São Paulo: Thomson Reuters Brasil, 2019.

CREMÉR, Jacques. **Competition policy for the digital era**: A report commissioned by the European Commission. 2019. Disponível em: <https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf>. Acesso em: 09 set. 2024.

DA SILVEIRA, Sérgio Amadeu. Economia da intrusão e modulação na Internet. **Liinc em Revista**, v. 12, n. 1, 2016.

DEUTSCHLAND. **Bundesanstalt für Finanzdienstleistungsaufsicht**. BaFin: Dark Patterns in Trading Apps unzulässig. Disponível em: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2022/meldung_2022_11_21_Dark_Patterns_in_TradingApps_Experten.html. Acesso em: 10 ago.

2024.

DIAS, Jean Carlos. **Direito Contratual no Ambiente Virtual**. Curitiba: Juruá, 2006.

DIAS, Lucia Ancona Lopez de Magalhães. **Publicidade e direito**. 2. ed. São Paulo: Revista dos Tribunais, 2013. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 12 ago. 2024.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais: elementos da formação da Lei Geral de Proteção de Dados**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, v. 12, n. 2, p. 91-108, 2011.

DRUCKER, P. F. **Sociedade pós-capitalista**. São Paulo: Pioneira, 1994.

DUROVIC, M.; POON, T. Consumer Vulnerability, Digital Fairness, and the European Rules on Unfair Contract Terms: What Can Be Learnt from the Case Law Against TikTok and Meta? **Journal of Consumer Policy**, v. 46, p. 361-375, 2023.

ECIPE. The EU Digital Markets Act: **Assessing the Quality of Regulation**. 2023. Disponível em: <https://ecipe.org>. Acesso em: 07 out. 2024.

EDPB. European Data Protection Board. **Guidelines 3/2022 on Dark patterns in social media platform interfaces**: How to recognise and avoid them. 21 de março de 2022.

FEATHERSTONE, Mike. **Undoing culture: globalization, postmodernism and identity**. London: Sage, 1995.

FERNANDES, Victor Oliveira. **Digital Markets Act (DMA) e o Direito da Concorrência na União Europeia**: o futuro finalmente chegou? Jota, julho de 2022.

FERRAZ, José Eduardo Junqueira. VIOLA, Mario. **A Internet e Sociedade: Direito ao esquecimento**. Disponível em: <https://itsrio.org/wp-content/uploads/2017/06/Direito-ao-esquecimento.pdf>. Acesso em: 30 de jun. 2024.

FILOMENO, José Geraldo Brito. **Manual de Direitos do Consumidor**. 5. ed. rev., atual. e ref. – São Paulo: Atlas, 2018.

FLETCHER, Amelia et al. **Prohibition of Self-Preferencing and Interoperability in Digital Platforms**. CEPR, 2021.

FLEURY, M. T. L. **As pessoas na organização**. São Paulo: Editora Gente, 2002.

FLUSSER, Vilém. **Filosofia da caixa preta: ensaios para uma futura filosofia da fotografia**. Rio de Janeiro: Relume Dumará, 2002.

FRANCE. **Commission Nationale de l'Informatique et des Libertés**. Cookies: la CNIL sanctionne GOOGLE à hauteur de 150 millions d'euros et FACEBOOK à hauteur de 60 milhões d'euros pour non-respect de la loi. Disponível em: <https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros-et-facebook-hauteur-de-60-millions>. Acesso em: 06 ago. 2024.

FRAZÃO, Ana. **A falácia da soberania do consumidor**: economia digital pode tornar o consumidor ainda mais vulnerável. Portal Jota, 08.12.2021. Disponível em: [\[https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/falacia-soberania-do-consumidor-08122021\]](https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/falacia-soberania-do-consumidor-08122021). Acesso em: 08 ago. 2024.

FRAZÃO, Ana. **Como conter as dark patterns**. Jota, 12 jun. 2024. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/como-conter-as-dark-patterns>. Acesso em: 08 set. 2024.

FURMAN, Jason. **Unlocking digital competition**: Report of the Digital Competition Expert Panel. 2019. Disponível em: <https://www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel>. Acesso em: 09 set. 2024.

GAMA, Hélio Zaghetto. **Curso de Direito do Consumidor**. 1ª Ed – 4ª tiragem. Rio de Janeiro: Forense, 2002.

GERADIN, Damien. **What is a digital gatekeeper?** Which platforms should be captured by the EC proposal for a digital market act? SSRN, 2021. Disponível em: <https://ssrn.com/abstract=3853991>. Acesso em: 08 set. 2024.

GRAY, Colin M. et al. **The dark (patterns) side of UX design**. In: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 2018. Disponível em: <https://doi.org/10.1145/3173574.317410>. Acesso em: 12 ago. 2024.

GRIMM, Dieter. **L'autorégulation régulée dans la tradition de l'État constitutionnel**. Trivium, Paris, n. 21, 2016.

HELBERGER, N.; LYNSKEY, O.; MICKLITZ, H.-W.; ROTT, P.; SAX, M.; STRYCHARZ, J. **EU Consumer Protection 2.0**: Structured Asymmetries in Digital Consumer Markets. BEUC, 2021. Disponível em: <https://www.beuc.eu/publications>. Acesso em: 03 set. 2024.

HOVENKAMP, Herbert. **Antitrust and innovation**: where we are and where we should be going. Antitrust Law Journal, Connecticut, n. 77, p. 749-751, 2011.

HYDE, R.; CARTWRIGHT, P. Exploring Consumer Detriment in Immersive Gaming Technologies. **Journal of Consumer Policy**, v. 46, p. 335-361, 2023.

IANNI, O. **Teorias da globalização**. Rio de Janeiro: Civilização Brasileira, 1996.

ITALIA. **Garante per la Protezione dei Dati Personali**. Newsletter 17/04/23 – Marketing: Garante privacy, no all'uso di modalità ingannevoli. Disponível em:

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870725>. Acesso em: 08 ago. 2024.

JABŁONOWSKA, Agnieszka et al. Exploring the Dark Patterns in Big Data: Big Data and Algorithms in the Digital Marketplace. **European Law Journal**, 2018.

JANDREY, Claudio L. Dark Patterns e seu Uso no Mercado de Consumo. **Revista de Direito do Consumidor**, v. 143, p. 231-257, set.-out. 2022.

KERBER, Wolfgang. Taming tech giants with a per se rules approach? The Digital Markets Act from the “rules vs. standard” perspective. **Concurrences Law Review**, v. 3, n. 1, p. 28–34, 2021.

KIRA, Beatriz. **As big techs e a nova onda de regulação digital ao redor do mundo**. JOTA, 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/as-big-techs-e-a-nova-onda-de-regulacao-digital-21072022>. Acesso em: 09 set. 2024.

KLEE, Antônia Espíndola Longoni. Comércio Eletrônico. 2. ed. São Paulo: **Revista dos Tribunais**, 2014.

KOTLER, P. **Administração de Marketing**. 10. ed. São Paulo: Prentice Hall Brasil, 2000.

KOTLIAR, D. M. Who Gets to choose? on the socio-algorithmic construction of choice. **Science Technology and Human Values**, v. 46, n. 2, p. 346-375, 2021. DOI: 10.1177/0162243920925147. Acesso em: 10 ago. 2024.

KUNER, Christopher. **Transborder Data Flows and Data Privacy Law**. Oxford: OUP Oxford, 2013.

LEMOS, André. **Cibercultura: tecnologia e vida social na cultura contemporânea**. Porto Alegre: Sulina, 2008.

LEMOS, Ronaldo. **Proteção de Dados e o Direito à Privacidade**. Rio de Janeiro: Zahar, 2018.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

LEYSER, Maria Fátima Vaquero Ramalho. **O comércio eletrônico e o Código de Defesa do Consumidor**. Consultor Jurídico, 24 de maio de 2021. Disponível em: <https://www.conjur.com.br/2021-mai-24/mp-debate-comercio-eletronico-codigo-defesa-consumidor/>. Acesso em: 07 jul. 2024.

LUGURI, Jamie; STRAHILEVITZ, Lior Jacob. **Shining a Light on Dark Patterns**. Journal of Legal Analysis, v. 13, p. 55, 2021. Disponível em: <https://academic.oup.com/jla/article/13/1/43/5876811>. Acesso em: 06 ago. 2024.

LUPIÁÑEZ-VILLANUEVA, F.; BOLUDA, A.; BOGLIACINO, F. et al. **Behavioural study on unfair commercial practices in the digital environment: dark patterns and manipulative personalisation – final report**, 2022. Comissão Europeia. Direção-

Geral da Justiça e dos Consumidores. Disponível em: <https://data.europa.eu/doi/10.2838/859030>. Acesso em: 07 ago. 2024.

LYOTARD, Jean François. **A condição pós-moderna**. 5. ed. Rio de Janeiro: José Olympio, 2009.

MACEIRA, M.; CARVALHO, F.; LIMA, V. Fatores demográficos na percepção do risco de compra pela Internet: o caso de um site brasileiro de venda de ingressos. **Revista Portuguesa e Brasileira de Gestão**, v. 10, n. 2, p. 92-101, 2011.

MARCOS, R. M. F. **Companhias Pombalinas**: contributo para a história das sociedades por acções em Portugal. Coimbra: Almedina, 1997.

MARTINS, Guilherme Magalhães. **Contratos eletrônicos de compra na internet e a proteção do consumidor**. Consultor Jurídico, São Paulo, 26 abr. 2017. Disponível em: <https://www.conjur.com.br/2017-abr-26/garantias-consumo-contratos-eletronicos-internet-protecao-consumidor>. Acesso em: 11 nov. 2024.

MARQUES, Claudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor**. São Paulo: Ed. RT, 2004.

MARQUES, Cláudia Lima. Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais. 9. ed. São Paulo: **Revista de Direito do Consumidor**, 2019.

MARQUES, Cláudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. Dark patterns e padrões comerciais escusos. **Revista de Direito do Consumidor**, São Paulo, v. 145, n. 32, p. 295-316, jan./fev. 2023.

MARQUES, Claudia Lima; MIRAGEM, Bruno. “Serviços simbióticos” do consumo digital e o PL 3.514/2015 de atualização do CDC. **Revista de Direito do Consumidor**, v. 132, p. 91-118, 2020.

MARQUES, Claudia Lima; MUCELIN, Guilherme. A vulnerabilidade digital do consumidor no ciberespaço: novas perspectivas para a proteção de dados pessoais e o papel do direito do consumidor. **Revista de Direito do Consumidor**, São Paulo, v. 134, p. 15-38, jan./fev. 2022.

MARQUES, Cláudia Lima. Confiança no comércio eletrônico e a proteção do consumidor. São Paulo: **Revista de Direito do Consumidor**, 2004.

MARQUES, Eduardo. **A desmaterialização do mundo**: tecnologia e sociedade. São Paulo: Annablume, 2004.

MARTIN, William J. **The Global Information Society**. Vermont: Brookfield, 1995.

MARTINS, Fernando Rodrigues; LIMA, Thainá Lopes Gomes. Da vulnerabilidade digital à curiosa “vulnerabilidade empresarial”. **Revista de Direito do Consumidor**, v. 128, p. 119-161, 2020.

MATHUR, Arunesh et al. **Dark patterns at scale**: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on Human-Computer Interaction, 2019. Disponível em: <https://doi.org/10.1145/3359183>. Acesso em: 04 ago. 2024.

MELO JUNIOR, Glauto Lisboa. Navegando por padrões obscuros: uma análise crítica da Lei dos Mercados Digitais (DMA) e da Lei dos Serviços Digitais (DSA) para a proteção dos consumidores on-line. **Revista da Faculdade de Direito da Universidade de Lisboa**, Lisboa, v. 64, n. 2, p. 545-573, 2023.

MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. **Revista de Direito do Consumidor**, v. 102, p. 1-30, 2020.

MENDES, Laura Schertel. Autodeterminação informativa: a história de um conceito. Pensar: **Revista de Ciências Jurídicas**, v. 25, n. 4, p. 34-58, out./dez. 2020.

MENDES, Laura Schertel; FONSECA, Gabriel C. Soares da. Proteção de dados para além do consentimento: tendências contemporâneas de materialização. **Revista Estudos Institucionais**, Rio de Janeiro, v. 6, n. 2, p. 507-533, maio/ago. 2020.

MIK, E. **The erosion of autonomy in online consumer transactions**. Law, Innovation and Technology, v. 8, n. 1, p. 1-38, 2016. DOI: 10.1080/17579961.2016.1161893. Acesso em: 13 ago. 2024.

MILHOMENS, Heitor Antunes. **Tutela da confiança e da vulnerabilidade na economia do compartilhamento**: empoderamento do consumidor digital e mitigação da vulnerabilidade estrutural na era do hiperconsumo. 2021. Dissertação (Mestrado em Direito) — Universidade Federal do Pará, Belém, 2021.

MIRAGEM, Bruno. **Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor**. Revista de Direito do Consumidor, São Paulo, vol. 125, p. 1-16, set.-out. 2019.

MIRAGEM, Bruno. **Curso de Direito do Consumidor**. 8. ed. São Paulo: Revista dos Tribunais, 2020.

MITCHELL, Andrew D.; MISHRA, Neha. Regulating cross-border data flows in a data-driven world: how WTO law can contribute. **Journal of International Economic Law**, v. 22, n. 1, p. 1-34, 2019.

MOREIRA, R. A. O Comércio Eletrônico, **Os Métodos de Pagamentos e os Mecanismos de Segurança**. FATEC: Jahu, 2016.

MOURA, R. M.; ALBERTIN, A. L. **Comércio eletrônico**: seus aspectos de segurança e privacidade. Revista de Administração de Empresas, vol. 38, n. 2, 1998. Disponível em: https://rae.fgv.br/sites/rae.fgv.br/files/artigos/10.1590_S0034-901998000200006.pdf. Acesso em: 02 jul. 2024.

MUCELIN, Guilherme; SILVA, Roberta Scalzilli. Neurodireitos e ultravulnerabilidade. **Revista de Direito do Consumidor**, v. 153, p. 225-256, maio/jun. 2024.

MUCELIN, Guilherme; JABRA, Alexandre. **Responsabilização de plataformas segundo STJ**: aplicação-fornecedora. Consultor Jurídico, 4 out. 2023. Disponível em: <https://www.conjur.com.br/2023-out-04/garantias-consumo-responsabilizacao-plataformas-segundo-stj2/>. Acesso em: 18 set. 2024.

NAKAMURA, R. R. **E-Commerce na Internet**: Fácil de Entender. São Paulo: Érica, 2001.

NANEHKARAN, Y. A. An introduction to electronic commerce. **International Journal of Scientific & Technology Research**, v. 2, n. 4, p. 190-193, 2013.

NEGROPONTE, Nicholas. **A vida digital**. São Paulo: Companhia das Letras, 1995.

NETO, José Luíz Castro et al. **Comércio eletrônico**: análise dos fatores críticos. *Business Review*, v. 9, p. 1-25, 2010.

NISSENBAUM, Helen. **Privacy as contextual integrity**. *Washington Law Review*, v. 79, p. 119-158, 2004. Disponível em: <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>. Acesso em: 07 set. 2024.

NORA, Simon; MINC, Alain. **A informatização da sociedade**. Rio de Janeiro: Fundação Getúlio Vargas, 1980.

NUNES, Rizzatto. **Curso de Direito do Consumidor**, 12ª Edição. Editora Saraiva, 2018.

O'BRIEN, J. A. **Sistemas de informação**: e as decisões gerenciais na era da Internet. 2. ed. São Paulo: Saraiva, 2004.

OCDE. **Dark commercial patterns**. Digital Economy Papers, n. 336, OECD Publishing, Paris, 2022.

OCDE. **Dark Commercial Patterns**. OECD Digital Economy Papers, No. 336, OECD Publishing, Paris, 2022. Disponível em: <https://doi.org/10.1787/44f5e846-en>. Acesso em: 11 ago. 2024.

OLIVEIRA, Tassiyara Onofre de. **Gestão de dados pessoais**: uma análise de casos concretos a partir do ordenamento jurídico brasileiro. 109 f. Dissertação (Mestrado em Gestão nas organizações aprendentes). Universidade Federal da Paraíba, João Pessoa, 2017.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). **Implementation toolkit on legislative actions for consumer protection enforcement co-operation**. OECD Digital Economy Papers, n. 310, 17 jun. 2021, 70 p. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/implementation-toolkit-on-legislative-actions-for-consumer-protection-enforcement-co-operation_eddc57-en. Acesso em: 14 ago. 2024.

RENZETTI, Bruno. **Digital Markets Act e o controle de estruturas no Brasil**. *Conjur*,

23 de outubro de 2022. Disponível em: <https://www.conjur.com.br/2022-out-23/bruno-renzetti-digital-markets-act-controle-estruturas/>. Acesso em: 18 set. 2024.

RIEFA, C.; SAINTIER, S. **Protecting Vulnerable Consumers in the Digital Single Market**. European Business Law Review, v. 33, p. 607-634, 2020.

RIFKIN, Jeremy. **A era do acesso**: a transição de mercados convencionais para networks e o nascimento de uma nova economia. São Paulo: Makron Books, 2001.

ROCHA, Rubens A.; ATZ, Neli. **Contratos eletrônicos**: o comércio eletrônico e a segurança jurídica. São Paulo: Saraiva, 2011.

RODOTÁ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Organização de Maria Celina Bodin de Moraes. Tradução: Danilo Doneada e Luciana Cabral Doneada. Rio de Janeiro: Renovar, 2008.

ROLIM, Fernanda Silva Scheffer. **Publicidade enganosa e abusiva**: a responsabilização e o fenômeno do dark patterns. 2023. Monografia (Bacharelado em Direito) – Universidade Federal do Rio Grande do Sul, Porto Alegre, 2023.

ROUVROY, Antoinette; POULLET, Yves. **The right to informational self-determination and the value of self-development**. In: GUTWIRTH, S. et al. (Ed.). Reinventing data protection? Dordrecht: Springer, 2009.

SAMPAIO, Marília de Ávila e Silva; JANDREY, Cláudio Luiz. Dark Patterns e seu uso no mercado de consumo. **Revista de Direito do Consumidor**, v. 143, p. 231-257, 2022.

SANTOS, E. B. dos; et al. **Marketing na Era Digital**. VI Jornada Acadêmica: Goiás, 2012.

SANTOS, Humberto Cunha dos. **A discussão de uma possível lei brasileira de regulação dos mercados digitais**: PL 2768/22 atribui à Anatel competências que o Digital Markets Act atribuiu à Comissão Europeia. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/como-a-regulacao-concorrencial-do-digital-markets-act-pode-inspirar-o-sbdc-25112022>. Acesso em: 12 set. 2024.

SANTOS, Humberto Cunha dos. **Digital Markets Act e suas implicações para a concorrência digital**. JOTA, 2022. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/digital-markets-act-25112022>. Acesso em: 09 set. 2024.

SANTOS, Roberta. A Regulação Internacional do Comércio Digital. **Revista de Direito Internacional**, v. 21, n. 1, p. 88-104, 2017.

SARAIVA NETO, Pery; FENILI, Maiara Bonetti. Novos marcos legais sobre proteção de dados pessoais e seus impactos na utilização e tratamento de dados para fins comerciais. **Revista de Estudos Jurídicos e Sociais - REJUS ON LINE [S.I.]**, v. 1, n. 1, dez. 2018.

SARMENTO, Daniel. **Liberdades Comunicativas e Direito ao Esquecimento na ordem constitucional brasileira**. Parecer divulgado no ano de 2015. Disponível em: <http://www.migalhas.com.br/arquivos/2015/2/art20150213-09.pdf>. Acesso em: 30 de jun. 2024.

SCANDIUZZI, Fernando. **Negócio eletrônico**: a logística no comércio eletrônico business to consumer (B2C) em empresas nacionais. 2005. Tese de Doutorado. Universidade de São Paulo. 2005.

SCHERHORN, G. The goal of consumer advice: Transparency or autonomy? **Journal of Consumer Policy**, v. 8, n. 2, p. 133-151, 1985. DOI: 10.1007/BF00380496. Acesso em: 9 ago. 2024.

SCHMIDT NETO, André Perin; AMARAL, Augusto Jobim do. Governar pela dívida: o crédito na era dos algoritarismos. **Revista de Direito do Consumidor**, São Paulo, vol. 143, ano 31, set./out. 2022.

SCHWABE, Jürgen; MARTINS, Leonardo. **Cinquenta anos de jurisprudência do Tribunal Constitucional Federal Alemão**. Montevideo: Konrad Adenauer Stiftung, 2005.

SCHWEITZER, Heike. **The Art to Make Gatekeeper Positions Contestable and the Challenge to Know What is Fair**: A Discussion of the Digital Markets Act Proposal. *Zeitschrift für europäisches Privatrecht*, v. 3, n. 1, p. 503–544, 2021.

SEBRAE. **Crescimento do e-commerce na pandemia é fruto de investimentos e muito trabalho**. Disponível em: <https://sebraepr.com.br/comunidade/artigo/crescimento-do-e-commerce-na-pandemia-e-fruto-de-investimentos-e-muito-trabalho>. Acesso em: 01 ago. 2024.

SHAFF, Adam. **A sociedade informática**: as consequências sociais da segunda revolução industrial. São Paulo: UNESP; Brasiliense, 1996.

SIDOU, J. M. Othon. **Direito do Consumidor**. 2. ed. Rio de Janeiro: Forense, 1977.

SILVA, Paula G. F. da. **Novas tecnologias, Big Tech e potenciais violações de direitos humanos: o caso dos sistemas de recomendação**. Dissertação (Mestrado em Direito) – Universidade Católica Portuguesa, Porto, 2021. Disponível em: <http://hdl.handle.net/10400.14/35771>. Acesso em: 06 ago. 2024.

SILVA, Tarcízio. **Racismo algorítmico**: inteligência artificial e discriminação nas redes digitais. Edições Sesc SP, 2022.

SILVEIRA, Sérgio Amadeu da; CASSINO, João Francisco; SOUZA, Joyce (orgs.). **Colonialismo de dados e modulação algorítmica**: tecnopolítica, sujeição e guerra neoliberal. São Paulo: Autonomia Literária, 2021.

SILVEIRA, Sérgio Amadeu. **A noção de exclusão digital diante das exigências de uma cibercidadania**. In: HETKOWSKI, Tânia Maria (Org.). *Políticas públicas e inclusão digital*. Salvador: EDUFBA, 2008.

SOARES, Ricardo Maurício Freire. **O princípio constitucional da dignidade da pessoa humana**: em busca do direito justo. São Paulo: Saraiva, 2010.

SOLOMON, M. R. **O Comportamento do Consumidor**: comprando, possuindo e sendo. 11. ed. Porto Alegre: Bookman, 2016.

SOUZA, Joyce; AVELINO, Rodolfo; Silveira, Sérgio Amadeu da (Org.). **A sociedade de controle**: manipulação e modulação nas redes digitais. São Paulo: Hedra, 2018.

SPERANZA, Henrique de Campos Gurgel. **Publicidade** enganosa e abusiva. Revista Síntese de Direito Civil e Processual Civil, Porto Alegre, n. 83, p. 43-45, 2020.

THALER, Richard H.; SUNSTEIN, Cass R. **Nudge**: Como tomar melhores decisões sobre saúde, dinheiro e felicidade. Rio de Janeiro: Objetiva, 2019.

TOFFLER, Alvin. **A terceira onda**. Rio de Janeiro: Editora Record, 1980.

TVERSKY, Amos; KAHNEMAN, Daniel. **Judgment under uncertainty**: heuristics and biases. Science, v. 185, ed. 4157, p. 1124-1131, 1974. Disponível em: <https://www.science.org/doi/10.1126/science.185.4157.1124>. Acesso em: 02 ago. 2024.

UNIÃO EUROPEIA. European Data Protection Board. **Guidelines 3/2022 on dark patterns in social media interfaces**: how to recognise and avoid them. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf. Acesso em: 10 ago. 2024.

UNIÃO EUROPEIA. Regulamento (EU) 2022/2065, de 19.10.2022. Artigo 67. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2065&from=EN>. Acesso em: 09 ago. 2024.

UNITED STATES OF AMERICA. Federal Trade Commission. **Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges**. Disponível em: <https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations>. Acesso em: 09 ago. 2024.

UNITED STATES OF AMERICA. Federal Trade Commission. **FTC Action Against Vonage Results in \$100 Million to Customers Trapped by Illegal Dark Patterns and Junk Fees When Trying to Cancel Service**. Disponível em: <https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-action-against-vonage-results-100-million-customers-trapped-illegal-dark-patterns-junk-fees-when-trying-cancel-service>. Acesso em: 07 ago. 2024.

VERBICARO, Dennis. O impacto do capitalismo de plataforma no agravamento da vulnerabilidade algorítmica do consumidor e do trabalhador. **Revista de Direito do Trabalho**, vol. 223, p. 277-305, 2022.

VERBICARO, Dennis; CALANDRINI, Jorge. A proteção da confiança do consumidor e a base do legítimo interesse na lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). **Revista de Direito do Consumidor**, vol. 139/2022, p. 73-99, jan.-fev., 2022.

VERBICARO, Dennis; MONTÃO, Vanessa Maria Dias. Empoderamento do consumidor no ambiente virtual. **Revista Jurídica (FURB)**, v. 26, p. e9910-e9910, 2022.

VERBICARO, Dennis; VIEIRA, Janaína. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. **Revista de Direito do Consumidor**, v. 134, p. 195-226, 2021.

VICENTE, Dário Moura. **Direito Comparado**. V. 1: introdução e parte geral. Coimbra: Almedina, 2008.

VIEIRA, Samira Santos Souza; DANTAS, Wellson Rosário Santos. Os desafios da proteção do consumidor no comércio eletrônico. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 10, n. 5, p. 2721-2732, 2024.

WAGNER, G.; EIDENMÜLLER, H. **Down by algorithms?** Siphoning rents, exploiting biases, and shaping preferences: Regulating the dark side of personalized transactions. *University of Chicago Law Review*, v. 86, n. 2, p. 581-609, 2019. DOI: 10.2139/ssrn.3160276. Acesso em: 14 ago. 2024.

WOOD, Ellen Meiksins. **A origem do capitalismo**. Rio de Janeiro: Editora Jorge Zahar Editor, 2001.

YEUNG, Karen. **‘Hypernudge’**: big data as a mode of regulation by design, 02.05.2016. *Information, Communication & Society* (2016) 1,19, TLI Think! Paper 28/2016. Disponível em: <https://ssrn.com/abstract=2807574>. Acesso em: 07 ago. 2024.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova estrutura do poder. Intrínseca, 2020.