SemeAd 2025
XXVIII Seminários em Administração

10, 11, 12, 13 e 14 de novembro de 2025
ISSN 2177-3866

LÁ VEM O GOLPE: UM ENSAIO TEÓRICO SOBRE A VULNERABILIDADE DO CONSUMIDOR FRENTE ÀS INOVAÇÕES DIGITAIS

ADELINE CARDOSO
EAUFBA - ESCOLA DE ADMINISTRAÇÃO DA UFBA

LÁ VEM O GOLPE: UM ENSAIO TEÓRICO SOBRE A VULNERABILIDADE DO CONSUMIDOR FRENTE ÀS INOVAÇÕES DIGITAIS

1 INTRODUÇÃO

Até meados dos anos 90 do século passado, a comodidade de comprar qualquer coisa fora das lojas físicas era comum através de catálogos, televendas ou revendedores (Magalhães, 2007; Silva, 2021). Com a liberação do uso comercial da internet em 1995 (Cruz, 2021), as relações comerciais foram ampliadas, com a disponibilidade gradual de múltiplos canais de venda e a integração crescente entre o ambiente on-line e o off-line (Okada & Porto, 2018). Desde então, o *e-commerce*, ou comércio eletrônico, segue em plena expansão, com metade da população brasileira realizando compras pela internet em 2024, segundo dados da pesquisa da Ebit Nielsen (Nielsen, 2025).

Apesar do aumento significativo de usuários conectados já na primeira década (Costa & Biachini, 2008), as preocupações com questões de segurança são um dos principais desafios do *e-commerce* desde o seu advento (Kovacs & Farias, 2004). O aperfeiçoamento da conectividade facilitou o compartilhamento de uma variedade de informações, transformando as relações e a comunicação global (Costa & Bezerra, 2024). Porém, criando ameaças. A otimização dos processos de compra e venda pela internet ao longo dos anos permitiu avanços na digitalização, a expansão massiva dos meios de pagamento eletrônicos e igualmente o aumento no volume e na natureza dos ataques à proteção do consumidor na internet (Chatrath et al., 2022; Pinheiro et al., 2025). Ao passo que as transações financeiras são facilitadas por aparelhos eletrônicos on-line, indivíduos e organizações criminosas se aproveitam do desconhecimento da população e das comodidades tecnológicas para aplicar golpes (Pinheiro et al., 2025).

O uso indevido da tecnologia favorece a intensificação de golpes aplicados no espaço virtual que prejudicam toda a sociedade, além de reduzir a confiança no comércio on-line (Ali et al., 2019). Além dos anúncios digitais falsos (Santiago & Araújo, 2022; Chatrath et al., 2022), fraudes em transações financeiras realizadas no ambiente eletrônico são amplamente noticiadas (Cruz, 2021; Chiusoli & Bonfim, 2020; Ali et al., 2019; Pinheiro et al., 2025). Conforme o Relatório de Identidade e Fraude 2025, da Serasa Experian, 51% dos brasileiros foram vítimas de fraudes em 2024. Destes, 54,2% teve perdas financeiras por golpes aplicados em cartões de crédito, transações fraudulentas via Pix ou boletos falsos e roubos de dados por mensagens (Serasa, 2025). Na maioria dos casos, os golpes digitais não são denunciados (Santini et al., 2025). A segurança e a privacidade lideram entre os principais atributos mais valorizados pelos consumidores nas compras e atividades no ambiente digital, de acordo com o estudo (Serasa, 2025).

Tal preocupação tem fundamento e exige uma transparência maior das empresas e profissionais de marketing em suas estratégias mercadológicas no ambiente digital (Ié et al., 2024). Com frequência, os consumidores são orientados a compartilhar informações pessoais na internet para acessar serviços on-line, atendendo ao interesse das empresas na coleta de dados, com o propósito de oferecer uma experiência mais personalizada aos seus clientes (Aiello et al., 2020; Ié et al., 2024). Para acessar ou manter o acesso a produtos e serviços, os dados pessoais se apresentam como uma condição inerente à participação do consumidor na economia digital (Marques & Mucelin, 2022).

Não obstante, essa prática expõe usuários digitais a riscos de violações de privacidade e manipulações de comportamentos por algoritmos (Ié et al., 2024), cujos danos podem se estender ao ambiente off-line (Pinheiro et al., 2025). Para que o acesso à informação ou serviço não lhe seja negado, o consumidor é levado a consentir no compartilhamento de seus dados,

com conhecimento e controle limitados quanto ao uso e práticas de marketing sobre os mesmos (Amin et al., 2025). Ainda que o *website* conceda a opção de não compartilhar, uma categoria mínima de dados – os chamados "cookies" – permite que empresas e profissionais de marketing rastreiem o consumidor on-line (Miller & Skiera, 2024). Assim, a falta de conhecimento ou controle sobre as práticas de marketing no uso das informações fornecidas gera no consumidor uma percepção de suscetibilidade a danos (Cloarec, 2022; Swani et al., 2022).

Decerto, o ambiente digital propicia o compartilhamento de dados a partir de diversos agentes econômicos, favorecendo as transações comerciais entre consumidores e empresas e entre os próprios usuários (Santiago & Araújo, 2022; Culiberg et al., 2024). Contudo, importa observar as práticas mercadológicas em todo o sistema de marketing que submetem o consumidor à vulnerabilidade, considerando as influências que o mercado exerce sobre a sua agência (Silva et al., 2021). Práticas como o rastreamento geográfico, o uso indevido de dados para o marketing secreto e a vigilância on-line do usuário por meio de aplicativos podem diminuir a confiança dos consumidores em uma empresa e provocar sentimentos de vulnerabilidade no consumo por canais digitais (Swani et al., 2022). Não obstante, o uso de padrões obscuros, que exploram vieses cognitivos como o efeito de ancoragem, enquadramento e desconto hiperbólico, podem prejudicar a autonomia do usuário ao reduzir a sua privacidade e afetar a sua tomada de decisão em *websites* ou aplicativos, independentemente de renda, idade ou escolaridade (Zac et al., 2025).

Neste contexto, cumpre aprofundar a investigação da vulnerabilidade do consumidor a golpes aplicados no espaço virtual face à crescente interconectividade dos consumidores e ao uso emergente das modernas tecnologias, incluindo a ascensão da inteligência artificial generativa (Gupta et al., 2024) e da internet das coisas – IoT (Amin et al., 2025). Uma vez que o marketing busca continuamente satisfazer as necessidades e atender às expectativas dos consumidores (Westrup & Paixão, 2023), a experiência centrada no usuário deve considerar o estado vulnerável dinâmico em que o consumidor se encontra à medida que novas tecnologias de marketing são introduzidas ao longo do tempo (Swani et al., 2022).

Isto posto, este ensaio pretende explorar como as práticas modernas de marketing influenciam na vulnerabilidade do consumidor no ambiente digital e como essas práticas reverberam na sofisticação dos golpes digitais frente às novas tecnologias. Dentro deste objetivo, busca colaborar com as pesquisas sobre o tema por meio de uma revisão narrativa de literatura, a partir de um enfoque multidisciplinar. Ou seja, com foco em pesquisas no campo do marketing e contribuições de estudos sobre a vulnerabilidade do consumidor, golpes financeiros aplicados por meio da internet e inovações digitais recentes sob a perspectiva de outras áreas do conhecimento, como Direito, Ciência de Dados, Tecnologia e Economia.

A pesquisa interdisciplinar se justifica pela diversidade de publicações acadêmicas pertinentes à investigação, fragmentada em diferentes disciplinas (Nguyen et al., 2025). A integração de múltiplas perspectivas traz relevância ao estudo e aprimora a compreensão da vulnerabilidade do consumidor a partir de um olhar mais amplo, podendo auxiliar numa investigação mais acurada das práticas de mercado no ambiente digital que podem causar danos ao consumidor (Ássimos et al., 2021; Riedel Et al., 2022; Basu et al., 2023).

Para alcançar o objetivo proposto, este ensaio se estrutura em quatro sessões além desta introdução. A segunda sessão se dedica a refletir sobre a vulnerabilidade do consumidor no ambiente digital. A terceira sessão reúne os tipos mais comuns de golpes financeiros aplicados na internet, abordados em artigos científicos nacionais e internacionais publicados nos últimos cinco anos, disponíveis nas plataformas Periódicos CAPES e Google Acadêmico. A quarta sessão destaca algumas das principais inovações digitais recentemente inseridas nos processos produtivos e na vida cotidiana, bem como as suas implicações na sofisticação dos golpes cibernéticos. Por fim, breves discussões são colocadas sobre o tema como conclusão do estudo nas considerações finais.

2 VULNERABILIDADE DO CONSUMIDOR NO ESPAÇO VIRTUAL

O estudo da vulnerabilidade do consumidor se caracteriza como uma área multidisciplinar, com contribuições de diversos campos do conhecimento. No Brasil, tem sua origem no Direito e interesse crescente entre profissionais e acadêmicos da área do marketing, especialmente nas últimas décadas (Silva et al., 2021). Como resultado das diferentes perspectivas teóricas na pesquisa em gestão e marketing, o conceito de vulnerabilidade do consumidor vem sendo construído com a colaboração coletiva de diversos autores (Khare & Jain, 2022; Basu et al., 2023).

Embora o termo tenha sido cunhado anteriormente, a definição da vulnerabilidade do consumidor ganhou destaque na literatura comportamental com o artigo seminal de Baker, Gentry e Rittenburg, publicado em 2005 (Khare & Jain, 2022). No estudo, a vulnerabilidade do consumidor foi estabelecida como um estado, transitório ou permanente, em que qualquer indivíduo está em desvantagem nas trocas de mercado ou a partir de mensagens e produtos de marketing. Neste contexto, a vulnerabilidade surge da interação entre estados e características individuais do consumidor e as condições externas, quando os objetivos de consumo podem ser prejudicados (Baker et al., 2005). Tal definição contribuiu para a compreensão do fenômeno e o desenvolvimento da estrutura conceitual do campo da vulnerabilidade do consumidor nos últimos anos (Khare & Jain, 2022).

A conceitualização da vulnerabilidade do consumidor como um estado difere da noção estática e categórica de vulnerabilidade decorrente de condições ou qualidades inerentes ao consumidor, comumente sustentada no Direito (Marques & Mucelin, 2022; Helberger et al., 2022). A compreensão de que qualquer indivíduo é suscetível à vulnerabilidade em algum momento na vida, independentemente de suas características pessoais, possibilita identificar os fatores externos e sociais que podem contribuir para tornar o consumidor vulnerável dentro de um contexto (Hill & Sharma; 2020; Helberger et al., 2022).

Em 2020, Hill e Sharma revisaram as definições acadêmicas existentes buscando construir uma estrutura que elencasse os antecedentes e consequências da vulnerabilidade do consumidor (Mende et al., 2024). Os autores consideraram investigar os recursos individuais, interpessoais e estruturais que potencializam o estado de vulnerabilidade do consumidor e as consequências com base nos seus mecanismos de enfrentamento em experiências de vulnerabilidade. O estudo contribuiu para ampliar o conceito, entendendo ainda a vulnerabilidade como um estado em que o consumidor pode sofrer danos devido à falta de acesso a recursos ou à falta de controle sobre os mesmos, tanto individuais e interpessoais quanto estruturais (Hill & Sharma, 2020).

A investigação da vulnerabilidade na pesquisa do consumidor não se limita, portanto, às características e condições individuais que podem levar o indivíduo a este estado (Strycharz & Duivenvoorde, 2021). Envolve fatores internos e externos que podem tornar os consumidores vulneráveis (Hill & Sharma, 2020). No ambiente digital, fatores internos podem desencadear a vulnerabilidade informacional frente às dificuldades do consumidor na obtenção e compreensão de informações, seja por características pessoais ou dificuldades no acesso à tecnologia (Cartwright, 2015). O despreparo técnico e intelectual, além da baixa proficiência em informática e de conhecimentos básicos para compreender a tecnologia on-line, sujeitam o consumidor contemporâneo a danos, por sua vulnerabilidade tática (Siqueira et al., 2021; Strycharz & Duivenvoorde, 2021; Nguyen et al., 2025).

Face à velocidade das inovações digitais, compete observar o estado dinâmico da vulnerabilidade que cada consumidor apresenta nas diversas fases da vida (Mende et al., 2024), posto que tecnologias algorítmicas podem reforçar a vulnerabilidade financeira, psicológica e física do consumidor on-line e off-line (Potnis et al., 2025). Assim, somam-se às diferenças quanto aos momentos de vida, as desigualdades sociais e falta de acesso a conhecimentos financeiros e econômicos básicos da população (Pinheiro et al., 2025), que caracterizam os

antecedentes da vulnerabilidade do consumidor nas transações financeiras digitais (Hill & Sharma, 2020).

Por sua vez, fatores externos incluem o acesso limitado à internet ou o ambiente no qual o consumidor interage, que também podem afetar a sua experiência de consumo (Baker et al., 2005; Hill & Sharma, 2020; Strycharz & Duivenvoorde, 2021) e envolver diferentes agentes do mercado (Silva et al., 2021). Neste ponto, a conectividade e facilitação dos processos de pagamento on-line favoreceram novos tipos de relações comerciais, nas quais os riscos a prejuízos podem ser intensificados (Helberger et al., 2022). É o caso da economia compartilhada, composta por consumidores, provedores de serviços e facilitadores, em que os usuários podem assumir papeis expandidos tanto como consumidores quanto como provedores simultaneamente (Culiberg et al., 2024). Os próprios sistemas que formam o mercado de consumo digital estão sujeitos à fragilidade na segurança a ataques e invasões ilícitas, caracterizando a vulnerabilidade estrutural do comércio eletrônico (Marques & Mucelin, 2022). Com isso, a diversidade de atores nas transações de compra e venda no ambiente digital exige que todos sejam dependentes de informações e orientados por tecnologias de otimização de dados (Helberger et al., 2022).

A disposição de dados, porém, não é necessariamente igualitária (Cloarec, 2022). Da mesma forma, as condições de acesso podem ser restritivas e ocultar práticas comerciais desleais (Helberger et al., 2022), posicionando o consumidor a uma condição de impotência (Rayburn et al., 2020). Para atingir a comunicação de marketing personalizada – PMC, empresas e profissionais de marketing se dedicam a compreender o comportamento do consumidor através de cliques, históricos de compra on-line e atividades de navegação (Ié et al., 2024). Tais atitudes, em conjunto com as informações demográficas e preferências do usuário, permitem que comerciantes e profissionais de marketing direcionem mensagens promocionais personalizadas no intuito de tornar o consumidor mais receptivo à venda de produtos e serviços (Chen et al., 2023). No entanto, mesmo que haja uma disposição do consumidor à personalização, sentimentos de vulnerabilidade podem surgir da exposição de dados à qual o consumidor não tem o controle (Cloarec, 2022; Ié et al., 2024).

Além disso, a coleta de dados em condições e termos fixados pelas empresas de forma unilateral cria uma assimetria de informações capaz de comprometer o empoderamento e poder de agência do consumidor (Cloarec, 2022), que se encontra em uma posição desfavorável (Baker et al., 2005). A fim de restabelecer o equilíbrio pela falta de controle suficiente sobre seus dados, consumidores podem prestar informações falsas ou criar identidades fictícias como um mecanismo de enfrentamento da vulnerabilidade e proteção no ambiente on-line (Cloarec, 2022; Hill & Sharma, 2020). Espaço construído no qual a sua liberdade difere do mundo físico (Marques & Mucelin, 2022). Assim mesmo, cada vez mais empresas e profissionais de marketing digital têm concentrado esforços na segmentação comportamental on-line para personalização de serviços, anúncios e preços (Strycharz & Duivenvoorde, 2021).

Isto posto, uma vez que os atores, acordos e modelos de negócios se alternam de forma rápida e dinâmica no comércio digital (Marques & Mucelin, 2022), a compreensão da vulnerabilidade do consumidor no atual cenário se tornou uma busca premente. Tanto pela dependência tecnológica crescente à qual a sociedade moderna está sujeita (Oliveira & Barroco, 2023; Stewart et al., 2024) quanto pela facilidade de acesso às informações, que implica na disseminação rápida de conteúdo, cuja precisão e integridade exigem cuidados constantes. Afinal, contrariamente, a disponibilidade de conteúdo na internet não garante a veracidade dos dados (Jaidka et al., 2025).

Logo, a rápida transformação nas relações comerciais a que o consumidor está exposto na "era da internet" evidencia a necessária atenção ao seu estado de vulnerabilidade a golpes e uma melhor compreensão das ameaças no espaço virtual (Cele & Kwenda, 2025; Pinheiro et al., 2025). Embora as empresas também sejam vulneráveis a perdas financeiras e interrupções

de serviços, os impactos de ataques cibernéticos aos consumidores podem se estender a traumas, à baixa confiança no mercado e à sua ruína financeira (Muammar et al., 2023).

3 A SOFISTICAÇÃO DOS GOLPES NA ERA DIGITAL

Diante da velocidade e alcance ampliados no ciberespaço, uma diversidade de técnicas fraudulentas cada vez mais sofisticadas pode atingir uma vasta quantidade de vítimas e causar prejuízos em larga escala (Bortot et al., 2024), expondo a população em geral a danos (Sarno & Black, 2023). Para o consumidor, os efeitos vão além da perda de bens, como dinheiro e informações pessoais (Costa & Bezerra, 2024). Podem influenciar ainda na sua capacidade de detectar fraudes e estabelecer confiança em comunicações reais, comprometendo o seu poder de agência nas atividades econômicas e o seu bem-estar (Robb & Wendel, 2023).

As principais formas de proteção integram desde o uso de senhas fortes à instalação de antivírus e *softwares* de segurança (Costa & Bezerra, 2024). Contudo, as modalidades de golpes virtuais contemplam técnicas ardilosas que confundem o consumidor, visto que os golpistas buscam aplicar estratégias semelhantes aos tipos de comunicação adotados por empresas e profissionais de marketing (Robb & Wendel, 2023). Diante da dificuldade de rastreamento no espaço virtual, os golpistas podem se passar por representantes de empresas e instituições, utilizando artifícios técnicos convincentes, como e-mails, imagens e até *websites* falsificados, para atrair a confiança de consumidores e extrair seus dados ou dinheiro (Chrysanthou et al., 2024).

Sob estas condições, a vulnerabilidade do consumidor se intensifica, tanto pela tendência das pessoas a acreditar na honestidade de outras pessoas, com base na probabilidade de serem enganadas (Sarno & Black, 2023), quanto pela associação a experiências que correspondam à premissa do golpe (DeLiema & Worley, 2023). Assim, a aparente legitimidade das tentativas de golpe contrasta com as táticas do marketing digital contemporâneo (Chrysanthou et al., 2024).

Ademais, a desconfiança do consumidor em mensagens e anúncios falsos confronta com a sua lealdade a uma marca ou produto. Ou seja, os níveis de relacionamento e confiança do consumidor com a fonte da mensagem recebida influenciam na sua credibilidade (Qureshi et al., 2024). Com isso, o uso de e-mails com domínio falso quase idêntico ao real (Chrysanthou et al., 2024) acompanhado de instruções imediatistas nos conteúdos fraudulentos são algumas das táticas engenhosas dos criminosos que costumam levar o consumidor ao engano (Garcia et al., 2023). Da mesma forma, a sua propensão a acreditar em conteúdos maliciosos tem forte relação com a sua intenção de compra (Qureshi et al., 2024), que pode ser identificada através de tecnologias algorítmicas, disponíveis em plataformas digitais aos usuários (Ié et al., 2024; Sakalauskas & Kriksciuniene, 2024; Santini et al., 2025).

É relevante acrescentar que, ainda que o consumidor se proteja de possíveis ataques, seja com a ajuda de *software*s ou treinando a sua alfabetização digital para detectar uma infinidade de enganos (Sarno & Black, 2023; Pinheiro et al., 2025), a diversidade e frequência dos golpes mudam com o tempo, acompanhando as dinâmicas sociais e políticas do momento (Robb & Wendel, 2023). Além disso, o Brasil ainda carece de legislação penal abrangente para todos os tipos de golpes financeiros aplicados com a obtenção de dados digitais (Pinheiro et al., 2025), podendo diferir de outras estruturas, como o sistema financeiro nacional, na identificação e tratamento dos mesmos (Bezzutti & Fernandes, 2022). Por esta razão, a responsabilidade digital corporativa, a transparência das informações por parte das empresas e sua conduta ética quanto à privacidade de dados são ações que podem auxiliar o consumidor na sua proteção e redução da sua vulnerabilidade (Cloarec, 2022).

Em suma, os golpes são tratados como artifícios enganosos praticados para obter informações ou dinheiro e causar prejuízos às vítimas (Bezzutti & Fernandes, 2022). Por sua diversidade, neste artigo serão destacadas separadamente algumas das técnicas utilizadas pelos

golpistas para aplicar golpes digitais e os tipos mais comuns de golpes financeiros praticados no ciberespaço nos últimos anos.

3.1 Técnicas usadas para a prática dos golpes

Os golpes digitais são fraudes praticadas no ambiente virtual em que as vítimas são abordadas por meios eletrônicos, como aplicativos de mensagens, e-mails, *websites*, mídias sociais ou mensagens de texto fraudulentas (Bezutti & Fernandes, 2022; Sarno & Black, 2023), além de mensagens de voz e ligações, com o uso de práticas discursivas persuasivas (Chrysanthou et al., 2024). Em posse dos dados, o golpista pode usar ou vender as informações fornecidas pela vítima (Garcia et al., 2023). Apesar da versatilidade, os golpes seguem uma metodologia, incluindo técnicas específicas (Bortot et al., 2024). Algumas se destacam abaixo.

3.1.1 *Hacking*

O termo *hacking* caracteriza o ato de acessar sistemas de computador, redes ou dispositivos eletrônicos de forma indevida para roubar, manipular ou corromper dados (Ameen & Faye, 2024). O *hacker* pode utilizar *software*s maliciosos para invadir sistemas visando a violação de dados, ou seja, para vazamento de informações pessoais sensíveis, protegidas ou confidenciais a pessoas não autorizadas (Muammar et al., 2023). Com o auxílio de *software*s, os dados podem ser roubados, leiloados ou expostos, comprometendo a privacidade das vítimas e favorecendo a aplicação de novos golpes (McIntosh et al., 2024).

3.1.2 Engenharia social

Os golpes financeiros utilizam engenharia social, um conjunto de técnicas de manipulação psicológica que se aproveitam da desatenção, incapacidade técnica ou desconhecimento das pessoas para extrair informações, espalhar vírus e causar danos aos usuários da internet (Bezutti & Fernandes, 2022). As técnicas não se limitam aos canais digitais, porém o espaço virtual costuma ser mais explorado do que as chamadas telefônicas, pois permitem maior alcance dos ataques (Robb & Wendel, 2023). De todo modo, os meios e técnicas podem ser usados simultaneamente conforme o tipo de golpe aplicado (Muammar et al., 2023). Com foco na persuasão, os golpistas podem realizar pesquisas de perfis e possíveis vulnerabilidades de usuários para selecionar as suas vítimas e estudar o comportamento dos consumidores, visando facilitar as abordagens e criar laços de confiança com os mesmos (Bezzutti & Fernandes, 2022).

3.1.2.1 *Phishing*

Em meio ao volume intenso de informações diariamente trocadas no espaço virtual, o consumidor pode se deparar com um e-mail aparentemente confiável e ser manipulado a clicar em um link ou arquivo malicioso, acreditando se tratar de uma mensagem legítima (Costa & Bezerra, 2024). Esta técnica caracteriza o *phishing*, cujo objetivo é enganar o usuário para obter suas informações pessoais, inclusive senhas e dados de cartões de crédito, por meio de e-mails (Garcia et al., 2023). O termo provem do verbo “pescar” em inglês (Bezzutti & Fernandes, 2022) e se constitui em etapas: entregar o “phishing” ao consumidor, persuadi-lo a tomar uma ação e se aproveitar ilegalmente dos dados coletados (Garcia et al., 2023). O processo inclui planejamento e configuração do golpe, com seleção da comunicação e dos dispositivos-alvo (Bortot et al., 2024).

Por e-mails, os golpistas utilizam a escalabilidade, visando atingir uma vasta quantidade de pessoas, e a personificação, em que se passam por uma loja ou instituições públicas ou privadas conhecidas para enganar os consumidores. Os e-mails normalmente contêm links que instalam *software*s maliciosos ou direcionam o consumidor a páginas falsas, para login ou fornecimento de informações confidenciais (Bortot et al., 2024).

3.1.2.2 *Vishing*

O *vishing* utiliza chamadas de voz para adquirir informações financeiras (Cele & Kwenda, 2025). Neste método, táticas, como a comunicação vocal, identificador de chamadas manipulado e *background* sonoro convincente, são utilizadas para transmitir uma falsa sensação de segurança e persuadir o consumidor a fornecer dados bancários, verificar conta, ativar serviços ou realizar transações financeiras (Bortot et al., 2024).

3.1.2.3 *Smishing*

O *smishing* se trata do uso de mensagens curtas ou SMS (Robb & Wendel, 2023) para aplicação dos golpes. As mensagens costumam ser bastante persuasivas e induzem os consumidores a uma ação imediata a partir de notificações falsas sobre necessidade de verificação de uma conta, violação de privacidade ou dados bancários congelados (Bortot et al., 2024). As mensagens são configuradas para envio em dias e horários estratégicos, com alto potencial de confundir o consumidor por conter mensagens curtas e diretas (Bezzutti & Fernandes, 2022).

3.1.2.4 *Spoofing*

O *spoofing* é uma tática que utiliza dados fictícios, como número de telefone, e-mail, *websites* e até imagens, falsificadas para dar mais autenticidade aos golpes. É uma técnica de falsificação de dados praticada normalmente junto com outros tipos de golpe (Muammar et al., 2023). O *spoofing* facial pode ser usado em perfis falsos e para burlar sistemas de reconhecimento facial (Ali et al., 2019).

3.1.2.5 Roubo de identidade

Parecido com o *spoofing*, no roubo de identidade o golpista usa as informações reais roubadas do consumidor para tirar proveito de benefícios destinados à vítima em instituições públicas ou privadas (Eleutiane & Oliveira, 2024). Com a posse dos dados, o golpista ainda consegue abrir contas, fazer empréstimos, realizar compras (Bortot et al., 2024) ou cometer novos golpes com a identidade da vítima (Muammar et al., 2023).

No Brasil, tem sido comum a prática de golpes envolvendo o roubo de identidade por meio do *WhatsApp*, aplicativo de mensagens instantâneas mais usado entre os brasileiros (Santini et al., 2025). A clonagem do aplicativo por meio de SMS permite que o golpista acesse a agenda de contatos da vítima e, se fazendo por ela, faz contato com novas vítimas solicitando informações ou pedindo ajuda financeira (Pinheiro et al., 2025). Outras redes sociais também têm sido utilizadas pelos golpistas, como *Facebook* e *Instagram* (Santini et al., 2025).

3.1.2.6 Extorsão por *softwares* maliciosos

Ataques por meio de *softwares* maliciosos, como *ransomware* ou *malware*, são aplicados por criminosos com o objetivo de bloquear a interface do usuário ou roubar dados e arquivos para chantagear vítimas e extorquir pagamentos de resgate (McIntosh et al., 2024). Os danos incluem a extorsão virtual diante do bloqueio de um determinado arquivo ou pasta ou ainda mais prejuízos, como abertura de contas e transferência de bens em caso de acesso indevido à assinatura digital das vítimas (Bortot et al., 2024). Em alguns ataques, trata-se de um arquivo executável, com semelhanças com um aplicativo comum, que se instala no dispositivo de maneira remota e vasculha pastas e arquivos do usuário sem o seu conhecimento (McIntosh et al., 2024).

Ultimamente, o *ransomware* tem sido utilizado para violação de dados e espionagem sem necessariamente extorquir as vítimas, afetando tanto consumidores quanto organizações públicas e privadas (McIntosh et al., 2024).

3.2 Tipos de golpes financeiros

Golpes financeiros não são uma novidade no Brasil, porém se aperfeiçoam na velocidade das inovações tecnológicas. Para a realização das transações on-line, os ataques que antes consistiam em transferências por DOC ou TED, atualmente se beneficiam de novas modalidades de pagamento, como o Pix (Pinheiro et al., 2025). Alguns tipos de golpes financeiros mais comuns aplicados pela internet são apresentados a seguir.

3.2.1 Anúncios e notícias falsas

Os anúncios e manchetes digitais falsas são utilizados na comunicação de uma variedade de ataques, como o *pishing*, e compartilhados a partir de diferentes meios para causar desinformação ou manipular consumidores à compra de determinados produtos (Sarno & Black, 2023). Anúncios fraudulentos buscam atrair as vítimas divulgando ofertas de produtos e serviços com descontos vantajosos, normalmente abaixo do mercado, para pagamento à vista (Bezzutti & Fernandes, 2022). Podem também oferecer ganhos rápidos e significativos (Pinheiro et al., 2025), como em investimentos (Muammar et al., 2023), ou direcionar o consumidor a *websites* falsos (Bezzutti & Fernandes, 2022). Os objetivos envolvem ainda persuadir o consumidor ao pagamento de produtos ou serviços diferentes do que foi anunciado ou que nunca serão entregues (Muammar et al., 2023).

Uma pesquisa sobre danos causados por publicidade enganosa nas plataformas da Meta, realizada pelo NetLab UFRJ, identificou 1.770 peças publicitárias com conteúdo fraudulento somente entre 10 e 21 de janeiro de 2025. Com frequência, os anúncios foram manipulados com o uso inadvertido de inteligência artificial, sendo compartilhados por 151 anunciantes em plataformas da Meta – *Facebook, Instagram* ou *WhatsApp*, e impulsionadas por ferramentas de segmentação com base em critérios demográficos, geográficos e de interesses dos usuários das plataformas (Santini et al., 2025). Um agravante deste golpe é que o conteúdo dissimulado e persuasivo dos anúncios falsos incentiva o seu compartilhamento rápido com a contribuição dos próprios usuários, que dão prosseguimento à distribuição em massa do conteúdo malicioso sem discernimento. A ação contribui para que os golpistas atinjam novos alvos facilmente, dada a natureza veloz de disseminação do ambiente virtual (Santiago & Araújo, 2022). Frente à dificuldade em detectar a legitimidade das informações, os consumidores tendem a compartilhar mais notícias falsas do que notícias reais (Sarno & Black, 2023).

3.2.2 Comunicados, notificações e suporte técnico

Os acessos às plataformas, *websites* e aplicativos exigem normalmente credenciais de acesso, que podem ter ou não prazo de validade. Em alguns serviços, é possível configurar notificações ao usuário de forma personalizada. Por meio de engenharia social, golpistas se aproveitam dessa conveniência para enviar notificações convincentes aos consumidores sobre atividades incomuns observadas na conta, direcionando-os para uma ação, como clicar em um link, baixar um arquivo ou ligar para um número de telefone (Bortot et al., 2024; Bezzutti & Fernandes, 2022). As alegações são semelhantes às usadas em outros tipos de golpes. Incluem sinalizar o usuário sobre a necessidade de validação de suas informações para evitar o encerramento da conta ou exigir o preenchimento de formulários de apelação para obter o acesso de volta a uma rede social (Chrysanthou et al., 2024). Notificações e comunicados falsos simulando entidades públicas são estratégias comuns, aplicadas principalmente após ocorrências de repercussão nacional, programas governamentais, campanhas de lançamento de produtos notáveis, como o Pix, ou mesmo em pandemias, como a COVID-19 (Santiago & Araújo, 2022; Sarno & Black, 2023). Os meios envolvem mensagens de texto, e-mails ou anúncios em redes sociais ou aplicativos de mensagens de texto (Bortot et al., 2024; Sarno & Black, 2023; Pinheiro et al., 2025; Santini et al., 2025).

3.2.3 Golpe do Impostor

O golpe do impostor é um tipo de golpe comum em que o golpista usa meios psicológicos, como se passar por uma pessoa ou empresa confiável, para ludibriar consumidores pessoalmente, por telefone ou por meios digitais (Robb & Wendel, 2023). Eles tentam manipular a vítima se apresentando como representantes ou autoridades de agências governamentais ou de instituições financeiras e, de forma persuasiva, alegam a necessidade de conferir detalhes da conta, ativar ou reativar serviços ou realizar transações fraudulentas (Bortot et al., 2024). Os consumidores também podem ser direcionados a uma falsa central de atendimento, quando são induzidos a informar seus dados, senhas e realizar transações bancárias ilícitas (Bezzutti & Fernandes, 2022), assim como podem ser abordados por um falso suporte técnico de empresas e serviços (Muammar et al., 2023). As técnicas incluem *phishing*, *smishing* ou *vishing*, sendo o público idoso alvo frequente de ligações para ataques com esse tipo de golpe (Bortot et al., 2024).

3.2.4 Golpe do Pix

O Brasil ocupa a segunda posição como maior mercado de pagamentos instantâneos do mundo, ficando somente atrás da Índia (Santini et al., 2025). O Pix permite a realização de transferências financeiras com menos de dez segundos (Pinheiro et al., 2025) e foi recentemente integrado ao *WhatsApp* (Santini et al., 2025). Embora ofereça diversos benefícios aos consumidores brasileiros nas transações on-line, também facilita para que os golpistas obtenham mais êxito nos golpes (Pinheiro et al., 2025). O Pix está entre os principais meios de pagamento explorados por criminosos para aplicar golpes financeiros no país (Serasa, 2025). Conforme o estudo do NetLab UFRJ, 79% das denúncias de golpes financeiros envolvendo o Pix partiram de plataformas da Meta – *Facebook*, *Instagram* ou *WhatsApp*, que oferecem serviços como Biblioteca de Anúncios e segmentação de usuários (Santini et al., 2025). Por meio de anúncios fraudulentos e *phishing*, golpistas coletam dados sensíveis do consumidor, podendo usar as informações para roubar ou registrar contas de bancos e chaves Pix em nome da vítima. Assim, nas transações financeiras, os valores que deveriam ser transferidos à vítima são direcionados às contas dos golpistas (Pinheiro et al., 2025).

3.2.5 Golpe do boleto falso

De acordo com o NetLab UFRJ, golpes com Pix e boletos são os que mais geram prejuízos no Brasil, superando os casos envolvendo cartão de crédito e roubo de celular (Santini et al., 2025). O boleto funciona como um instrumento utilizado pelos golpistas em *websites* falsos e anúncios fraudulentos compartilhados pelos meios digitais, assim como podem ser falsificados para a cobrança ilícita de produtos e serviços legítimos, apresentando layout e informações idênticas à cobrança original. Porém, credor diferente (Bezzutti & Fernandes, 2022).

3.2.6 Clonagem de cartões de crédito ou uso por terceiros

As clonagens de cartões de crédito ocorrem por meio de diversos tipos de golpes. Por exemplo, através de *websites* falsos, projetados exclusivamente para coleta de informações das vítimas, o consumidor pode fornecer dados pessoais e bancários pensando se tratar de um *website* de uma loja legítima ou de uma instituição pública ou privada conhecida (Pinheiro et al., 2025). Em alguns casos, o *website* direciona o consumidor a entrar em contato com uma central de telefone falsa, quando é convencido por golpistas a fornecer seus dados (Ali et al., 2019). De acordo com a Serasa, o uso indevido do cartão de crédito lidera o ranking entre os tipos de golpes mais frequentes no Brasil (Serasa, 2025).

Os golpes ainda envolvem as compras por *websites* e aplicativos com opção de *delivery*, quando o cartão é clonado pela maquininha de pagamento do entregador. Também podem ser

usados em conjunto com outros golpes, como o golpe do impostor, em que golpistas se fazem de funcionários de instituições financeiras, instituições públicas ou serviços de logística para entrega de encomendas falsas (Pinheiro et al., 2025; Chrysanthou et al., 2024).

3.2.7 Mídias sociais

As modernas plataformas de redes sociais são frequentemente utilizadas para publicidade e promoção de produtos, de serviços e de profissionais, sendo alvo recorrente de golpistas dada a falta de transparência de suas políticas aos usuários e a baixa regulação do ambiente digital e (Santini et al., 2025). Tanto o *phishing* quanto o *smishing* podem ser aplicados em redes sociais, por meio de mensagens privadas, postagens públicas ou anúncios falsos, cuja segmentação através de ferramentas disponíveis nas plataformas permite alcançar perfis diversos ou específicos de vítimas (Garcia et al., 2023).

4 INOVAÇÕES DIGITAIS RECENTES: OPORTUNIDADES E RISCOS

Décadas de avanços científicos, maior poder computacional e novas tecnologias contribuíram para o desenvolvimento da inteligência artificial – IA, que pode ser resumida como uma tecnologia que torna máquinas e computadores capazes de executar tarefas simulando o raciocínio humano (Gupta et al., 2024; Scott, 2024). Dentro do vasto domínio da IA, encontram-se técnicas como aprendizado de máquina, aprendizado profundo e processamento de linguagem natural – PNL, que permitem a criação de uma variedade de inovações (Gupta et al., 2024). Um exemplo são os *chatbots* de inteligência artificial, utilizados para facilitar o atendimento de consumidores, proporcionando comunicação e acesso a informações de forma mais eficiente (Arce-Urriza et al., 2025).

Com a ajuda de tecnologias de inteligência artificial, a interconectividade permitiu o desenvolvimento e crescimento exponencial da Internet das Coisas – IoT, um conjunto de aplicações que possibilitam a conexão entre coisas, de máquinas a equipamentos vestíveis. Alguns exemplos são assistentes virtuais, como *Siri* e *Alexa*, relógios inteligentes ou aplicativos com GPS, como *Waze* e *Google Maps*, entre outros serviços e dispositivos presentes no cotidiano das pessoas. Para fornecer um serviço personalizado e aprimorar a inteligência empresarial, os prestadores coletam uma grande variedade de dados, incluindo hábitos dos usuários e informações pessoais, ambientais e de saúde, sem a devida transparência ou consentimento dos consumidores (Amin et al., 2025).

Somam-se às questões éticas da coleta desses dados, o uso indevido para publicidade não solicitada ou discriminação de preços. Outrossim, a resposta habitual a esses dispositivos e falta de conscientização quanto ao seu funcionamento podem levar o consumidor a, irrefletidamente, compartilhar informações pessoais confidenciais que, em casos de vazamento de dados por ataques cibernéticos ou distribuição indevida a terceiros, podem lhe causar danos inestimáveis (Amin et al., 2025).

Discussões quanto aos impactos das inovações digitais também destacam o rápido avanço e potencial transformador da inteligência artificial generativa na sociedade contemporânea (Scott, 2024). De forma simplificada, a IA generativa se concentra no treinamento de modelos capazes de aprender padrões complexos a partir de dados existentes para gerar conteúdos novos e realistas na forma de literatura, imagem, músicas ou vídeos (Gupta et al., 2024). O desenvolvimento e ascensão dessa tecnologia implica em transformações significativas nas estratégias de marketing centradas no consumidor, beneficiando na redução de custos, otimização do tempo, análise e resumo de dados complexos, além de auxiliar na criação de conteúdos criativos, personalização e reconhecimento emocional (Arce-Urriza et al., 2025). A capacidade de criação e personalização permite que marcas e empresas aprimorem o relacionamento com seu público, seja no atendimento ágil e individualizado ou por meio de materiais de marketing personalizados (Gupta et al., 2024).

Em contrapartida, a adoção e popularização de tecnologias avançadas como a IA generativa despertam preocupações quanto às implicações do uso desordenado dessas tecnologias para o bem-estar do consumidor no ambiente on-line, uma vez que a modelagem generativa pode ser usada para a fabricação de conteúdos falsos e maliciosos (Gupta et al., 2024). O levantamento de anúncios fraudulentos em redes sociais realizado pelo NetLab UFRJ apontou que mais de 70% das peças publicitárias foram adulteradas com o uso de inteligência artificial, por meio de ferramentas que tornam os conteúdos mais convincentes (Santini et al., 2025). Adicionalmente, o potencial de inteligência artificial e automação favorecem o ataque mais rápido e eficiente de invasões de *ransomware*, dificultando a detecção e resposta das organizações para evitar danos (McIntosh et al., 2024). Assim, a velocidade e integração dessas inovações no ambiente digital aliadas à baixa regulamentação e crescente mercantilização da informação podem sujeitar o consumidor a riscos e afetar a sustentabilidade dos negócios on-line a longo prazo (Amin et al., 2025).

5 CONSIDERAÇÕES FINAIS

Este ensaio buscou refletir sobre as práticas mercadológicas atuais que podem elevar a vulnerabilidade do consumidor a golpes financeiros digitais em uma sociedade progressivamente dependente da tecnologia. Diante do exposto, os estudos sobre a vulnerabilidade do consumidor no ambiente digital sugerem que as preocupações quanto às estratégias mercadológicas para alcance dos objetivos corporativos devem considerar as implicações éticas de suas práticas para o bem-estar do consumidor.

Decerto, o uso de inovações digitais amplamente disponíveis e em rápida expansão amplia a competitividade entre os agentes econômicos, exigindo um conjunto de ações para que as empresas se mantenham relevantes em um cenário de múltiplas opções. No entanto, os impactos de tais ações na vulnerabilidade do consumidor podem reduzir a sua confiança nas relações comerciais on-line e o sujeitar a prejuízos diante da falta de transparência das empresas.

Outrossim, a exposição massiva de informações a partir da coleta por meio de inovações digitais eleva as preocupações da sociedade quanto às ameaças de ataques cibernéticos, que causam perdas financeiras ao consumidor e geram vulnerabilidades na sua relação com as instituições. Por sua vez, a posse de uma diversidade de dados pessoais dos consumidores torna instituições públicas e privadas alvos potenciais de ataques cibernéticos, exigindo maior transparência das organizações e terceiros quanto à coleta, processamento e proteção das informações dos consumidores.

Sendo indispensável a conscientização dos usuários sobre o uso e os riscos das facilidades emergentes, a intervenção do marketing na orientação dos consumidores para o consumo seguro também pode contribuir na redução das vulnerabilidades no ciberespaço. Não havendo conhecimento adequado dos usuários quanto aos riscos da exposição de dados na internet a partir do consumo das novas tecnologias, toda a sociedade se torna vulnerável a danos irreparáveis.

Portanto, são necessários esforços conjuntos, que envolvam consumidores, a indústria privada e o setor público nas ações preventivas, que podem incluir publicidade antifraude precisa para conhecimento e alerta aos consumidores. Ademais, faz-se necessário um empenho maior do setor público na regulamentação urgente do ambiente digital, visto que a popularização das inovações digitais propicia facilidades tanto para as atividades do marketing quanto para as práticas fraudulentas, intensificando e refinando os golpes financeiros digitais.

Por fim, sem a intenção de desconsiderar os inúmeros benefícios da inteligência artificial e suas ramificações para a sociedade, acredita-se que as reflexões levantadas neste estudo agregam conhecimento e apresentam contribuições para a compreensão sob múltiplas perspectivas do estado de vulnerabilidade do consumidor na era digital.

REFERÊNCIAS

Aiello, G., Donvito, R., Acuti, D., Grazzini, L., Mazzoli, V., Vannucci, V., & Viglia, G. (2020). Customers' willingness to disclose personal information throughout the customer purchase journey in retailing: The role of perceived warmth. *Journal of Retailing*, Elsevier, vol. 96(4), pages 490-506. https://doi.org/10.1016/j.jretai.2020.07.001

Ali, M. A., Azad, M. A., Centeno, M. P., Hao, F., & Moorsel, A. van. (2019). Consumer-facing technology fraud : economics, attack methods and potential solutions. *Future Generation Computer Systems*, 100. pp. 408-427. https://doi.org/10.1016/j.future.2019.03.041

Ameen, S., & Faye, A. (2024). Role of media – social, electronic, and print media – in mental health and wellbeing. *Indian Journal of Psychiatry* 66(Suppl 2):p S403-S413. https://doi.org/10.4103/indianjpsychiatry.indianjpsychiatry_611_23

Amin, M. A. S., Kim, S., Rishat, M. A. S. A., Tang, Z., & Ahn, H. (2025). A Systematic Literature Review of Privacy Information Disclosure in AI-Integrated Internet of Things (IoT) Technologies. *Sustainability*, 17(1), 8. https://doi.org/10.3390/su17010008

Arce-Urriza, M., Chocarro, R., Cortiñas, M., & Marcos-Matás, G. (2025). From familiarity to acceptance: The impact of Generative Artificial Intelligence on consumer adoption of retail chatbots. *Journal of Retailing and Consumer Services*. https://doi.org/10.1016/j.jretconser.2025.104234

Ássimos, B. M., Luna, G., & Pinto, M. R. (2021). Por uma abordagem holística da vulnerabilidade do consumidor: uma breve discussão seguida por uma análise bibliométrica do tema. *SEMEAD XXIV*. https://login.semead.com.br/24semead/anais/arquivos/453.pdf?

Baker, S. M., Gentry, J. W., & Rittenburg, T. L. (2005). Building understanding of the domain of consumer vulnerability. *Journal of Macromarketing*, 25(2), pp. 128–139. https://doi.org/10.1177/0276146705280622

Basu, R., Kumar, A., & Kumar, S. (2023). Twenty-five years of consumer vulnerability research: Critical insights and future directions. *Journal of Consumer Affairs*, 57(1), 673–695. https://doi.org/10.1111/joca.12518

Bezzutti, M. C., & Fernandes, E. A. (2022). Os golpes no sistema financeiro na ótica da engenharia social. *Mercosur en Revista Educación, Tecnología y Sustentabilidad*, Asunción, v. 2, n. 2, p. 65-87. https://ojs.uep.edu.py/index.php/mercosur/article/view/315

Bortot, E. N., Franz, L. M., Guerra, M. V., Bernartt, M. de L., & Godoy, W. I. (2024). Teias de engano: uma análise dos riscos e estratégias de prevenção aos golpes cibernéticos praticados contra pessoas idosas na era digital. *Contribuciones a las Ciencias Sociales*, 17(13), e13534. https://doi.org/10.55905/revconv.17n.13-171

Cartwright, P. (2015). Understanding and Protecting Vulnerable Financial Consumers. *J Consum Policy* 38, 119–138. https://doi.org/10.1007/s10603-014-9278-9

Cele, N.N., & Kwenda, S. (2025). "Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review", *Journal of Financial Crime*, Vol. 32 No. 1, pp. 31-48. https://doi.org/10.1108/JFC-10-2023-0263

Chatrath, S. K., Batra, G. S., & Chaba, Y. (2022). Handling consumer vulnerability in e-commerce product images using machine learning. *Heliyon*, 8(9), e10743. https://doi.org/10.1016/j.heliyon.2022.e10743

Chrysanthou, A., Pantis, Y., & Patsakis, C. (2024). The anatomy of deception: Measuring technical and human factors of a large-scale phishing campaign. *Computers & Security* 140 (2024). Elsevier. https://doi.org/10.1016/j.cose.2024.103780

Cloarece, J. (2022). Privacy controls as an information source to reduce data poisoning in artificial intelligence-powered personalization. *Journal of Business Research*. Vol. 152, p. 144-153. https://doi.org/10.1016/j.jbusres.2022.07.045

Chen, S., Wu, Y, Deng, F., & Zhi, K. (2023). How does ad relevance affect consumers' attitudes toward personalized advertisements and social media platforms? The role of information co-ownership, vulnerability, and privacy cynicism. *Journal of Retailing and Consumer Services*. Elsevier, 73. https://doi.org/10.1016/j.jretconser.2023.103336

Chiusoli, C. L.; Bonfim, R. S. (2020). E-commerce: o comportamento de compras on-line na percepção dos consumidores. *Revista Administração em Diálogo* - RAD, v. 22, n. 2, p. 115–133. http://dx.doi.org/10.23925/2178-0080.2020v22i2.46989

Costa, L. S., & Bezerra, M. A. A. (2024). Os desafios da investigação criminal de crimes virtuais na era digital. *Revista Ibero-Americana de Humanidades, Ciências e Educação*, 10(10), 2111–2132. https://doi.org/10.51891/rease.v10i10.16023

Costa, P. da., & Bianchini, D. (2008). Caracterização da demanda futura de usuários da internet no Brasil: uma contribuição para o desenvolvimento de políticas governamentais de inclusão digital e acesso a internet. *JISTEM - Journal of Information Systems and Technology Management*, 5(1), 135–162. https://doi.org/10.4301/S1807-17752008000100007

Cruz, W. L. de M. (2021). Crescimento do e-commerce no Brasil: desenvolvimento, serviços logísticos e o impulso da pandemia de Covid-19. *GeoTextos*, 17(1). https://doi.org/10.9771/geo.v17i1.44572

Culiberg, B., Kos Koklic, M., Kukar-Kinney, M., & Vida, I. (2024). Vulnerability and perceived risks in the peer-to-peer sharing economy. *International Journal of Consumer Studies*, 48(2), e13028. https://doi.org/10.1111/ijcs.13028

DeLiema, M., Volker, J., & Worley, A. (2023). Consumer experiences with gift card payment scams: Causes, consequences, and implications for consumer protection. *Victims & Offenders*, 18(7), 1282–1310. https://doi.org/10.1080/15564886.2023.2244468

Eleutiane, J., & Oliveira, A. T. B. (2024). Furto de identidade. Revista Mundo em Movimento. v. 1, n. 1. https://doi.org/10.5281/zenodo.14618047

Garcia, K. R., Ammons, J., Xu, X., & Chen, J. (2023). Phishing in Social Media: Investigating Training Techniques on Instagram Shop. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 67(1), 1850-1855. https://doi.org/10.1177/21695067231192588

Gupta, R., Nair, K., Mishra, M., Ibrahim, B., & Bhardwaj, S. (2024). Adoption and impacts of generative artificial intelligence: Theoretical underpinnings and research agenda. *International Journal of Information Management Data Insights*, 4(1), 100232. https://doi.org/10.1016/j.jjimei.2024.100232

Helberger, N., Sax, M., Strycharz, J. et al. (2022). Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability. *J Consum Policy* 45, 175–200. https://doi.org/10.1007/s10603-021-09500-5

Hill, R., & Sharma, E. (2020). Consumer Vulnerability. *Journal of Consumer Psychology*, 30(3), pp. 551-570. https://doi.org/10.1002/jcpy.1161

Ié, O. A., Araújo, A. dos S., & Nunes, M. S. C. (2024). Propaganda digital e algoritmos e suas implicações nas escolhas dos usuários no ambiente online. *Encontros Bibli*, 29, e96375. https://doi.org/10.5007/1518-2924.2024.e96375

Jaidka, K., Chen, T., Chesterman, S., Hsu, W., Kan, M. Y., Kankanhalli, M. ... & Yue, A. (2025). "Misinformation, disinformation, and generative AI: Implications for perception and policy," *Digital Government: Research and Practice*, vol. 6, no. 1, pp. 1-15. https://doi.org/10.1145/3689372

Khare, A., & Jain, R. (2022). "Mapping the conceptual and intellectual structure of the consumer vulnerability field: A bibliometric analysis," *Journal of Business Research*, Elsevier, vol. 150(C), pages 567-584. https://doi.org/10.1016/j.jbusres.2022.06.039

Kovacs, M. H., & Farias, S. A. de. (2004). Dimensões de riscos percebidos nas compras pela internet. *RAE Eletrônica*, 3(2). https://doi.org/10.1590/S1676-56482004000200013

Magalhães, A. S. (2007). E-commerce e e-banking no Brasil: uma perspectiva do usuário. *Dissertação de Mestrado*, USP. https://doi.org/10.11606/D.12.2007.tde-21012008-145601

Muammar, S., Shehada, D. & Mansoor, W. (2023). Digital Risk Assessment Framework for Individuals: Analysis and Recommendations, *IEEE Access*, vol. 11, pp. 85561-85570. https://doi.org/10.1109/access.2023.3293062

Marques, C. L.; Mucelin, G. (2022). Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor. *Civilística*, a. 22, n. 3. https://civilistica.emnuvens.com.br/redc/article/view/872/649

McIntosh, T., Susnjak, T., Liu, T., et al. (2024). Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration. *ACM Computing Surveys*. 57. 1. https://doi.org/10.1145/3691340

Mende, M., Bradford, T.W., Roggeveen, A.L. et al. (2024). Consumer vulnerability dynamics and marketing: Conceptual foundations and future research opportunities. *Journal of the Academy of Marketing Science*. 52, 1301–1322. https://doi.org/10.1007/s11747-024-01039-4

Miller, K. M., & Skiera, B. (2024). Economic consequences of online tracking restrictions: Evidence from cookies. *International Journal of Research in Marketing*. Elsevier, 41, 241-264. https://doi.org/10.1016/j.ijresmar.2023.10.001

Nguyen, T. T., Nguyen, H. T., Nguyen, A. V., Tran P. T., Mai, H. N., & Pham, T. V. A. (2025). Consumers' Vulnerability and E-commerce purchase behavior: A serial mediation model. *Telematics and Informatics Reports*. Elsevier, vol, 18. https://doi.org/10.1016/j.teler.2025.100215

Nielsen, E (2025). Webshoppers 51ª ed. São Paulo. https://company.ebit.com.br/webshoppers/webshoppersfree

Okada, S., & Porto, R. (2018). Comportamento do Consumidor em Canais Cruzados: Modelo de Mediação-Moderada nas Compras Online/Offline. *Revista De Administração Contemporânea*, 22(4), 510–530. https://doi.org/10.1590/1982-7849rac2018170053

Oliveira, F. A. F. de., & Barroco, S. M. S. (2023). Revolução tecnológica e smartphone: considerações sobre a constituição do sujeito contemporâneo. *Psicologia Em Estudo*, 28, e51648. https://doi.org/10.4025/psicolestud.v28i0.51648

Pinheiro, J. M. L., Santos, L. F. G., Alves, G., Pereira, R. S., & Silva, W. J. B. (2025). A potencialidade da educação financeira crítica frente aos golpes financeiros. *ARACÊ*, 7 (5), 23775-23798. https://doi.org/10.56238/arev7n5-166

Potnis, D., Tahamtan, I., & McDonald, L. (2025). Negative consequences of information gatekeeping through algorithmic technologies: An Annual Review of Information Science and Technology (ARIST) paper. *Journal of the Association for Information Science and Technology*, 76(1), 262–288. https://doi.org/10.1002/asi.24955

Qureshi, M. A., Shahzadi, S., & Hussain, T. (2024). Exploring the Role of Influencers' Perceived Fraud Between Influencers' Credibility and Consumer Purchase Intentions. International *Journal of Professional Business Review*, 9(1), e04313. https://doi.org/10.26668/businessreview/2024.v9i1.4313

Rayburn, S. W., Mason, M. J., & Volkers, M. (2020). Service Captivity: No Choice, No Voice, No Power. *Journal of Public Policy & Marketing*, 39(2), 155-168. https://doi.org/10.1177/0743915619899082

Riedel, A., Messenger, D., Fleischman, D., & Mulcahy, R. (2022), "Consumers experiencing vulnerability: a state of play in the literature", *Journal of Services Marketing*, Vol. 36 No. 2, pp. 110-128. https://doi.org/10.1108/JSM-12-2020-0496

Robb, C.A., & Wendel, S. (2023). Who Can You Trust? Assessing Vulnerability to Digital Imposter Scams. *J Consum Policy*, 27–51. https://doi.org/10.1007/s10603-022-09531-6

Sakalauskas, V., & Kriksciuniene, D. (2024). Personalized Advertising in E-Commerce: Using Clickstream Data to Target High-Value Customers. *Algorithms*, 17(1), 27. https://doi.org/10.3390/a17010027

Santiago, A. H. R., & Araújo, J. (2022). Prática discursiva de desinformação: distribuição de anúncios digitais falsos em mídias sociais. *Revista Linguagem em Foco*, v.14, n.2, p. 49-67. https://doi.org/10.46230/2674-8266-14-9374

Santini, R. M., Salles, D., Mattos, B., et al. (2025). Danos causados pela publicidade enganosa na Meta: Anúncios fraudulentos promovem desinformação sobre o Pix para lesar cidadãos brasileiros. *NetLab – Laboratório de Estudos de Internet e Redes Sociais*. https://netlab.eco.ufrj.br/post/danos-causados-pela-publicidade-enganosa-na-meta

Sarno, D. M., & Black, J. (2023). Who Gets Caught in the Web of Lies?: Understanding Susceptibility to Phishing Emails, Fake News Headlines, and Scam Text Messages. *Human Factors*, 66(6), 1742-1753. https://doi.org/10.1177/00187208231173263

Scott, I. (2024). Rising to Meet the Challenge of Generative AI. *Journal of Legal Studies Education*, v. 41, n. 1, p. 29–37. https://doi.org/10.1111/jlse.12141

Serasa Experian (2025). Relatório de Identidade Digital e Fraude 2025. https://www.serasaexperian.com.br/images-cms/wp-content/uploads/2025/03/Relatorio-de-Identidade-Digital-e-Fraude-2025-Serasa-Experian.pdf

Silva, L. F. B. (2021). Publicidade comportamental e vigilância: pressupostos para responsabilização civil dos sites de redes sociais na internet. *Dissertação de Mestrado*, UFU. http://doi.org/10.14393/ufu.di.2021.328

Silva, R. O. D., Barros, D. F., Gouveia, T. M. D. O. A., & Merabet, D. D. O. B. (2021). Uma discussão necessária sobre a vulnerabilidade do consumidor: avanços, lacunas e novas perspectivas. *Cadernos EBAPE.BR*, 19(1), 83–95. https://doi.org/10.1590/1679-395120200026

Siqueira, O. N., Contin, A. C., Barufi, R. B., & Lehfeld, L. de S. (2021). A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. *Revista Eletrônica Esquiseduca*, 13(29), 236–255. https://doi.org/10.58422/repesq.2021.e1029

Stewart, K., Perren, R., Chambers, C., & Zulauf, R. (2024). In tech we rely: How technology dependence fuels consumer vulnerability. Journal of Consumer Affairs. *Advance Online Publication*. https://doi.org/10.1111/joca.12610

Strycharz, J., & Duivenvoorde, B. (2021). The exploitation of vulnerability through personalised marketing communication: are consumers protected? *Internet Policy Review*, 10(4). https://doi.org/10.14763/2021.4.1585

Swani, K., Milne, G. R., & Slepchuk, A. N. (2022). Revisiting Trust and Privacy Concern in Consumers' Perceptions of Marketing Information Management Practices: Replication and Extension. *Journal of Interactive Marketing*, 56(1), 137-158. https://doi.org/10.1016/j.intmar.2021.03.001

Westrup, A. C., & Paixão, P. B. S. (2023). Taggers: Marketing 4.0 e o case da TAG. Intercom: *Revista Brasileira De Ciências Da Comunicação*, 46, e2023137. https://doi.org/10.1590/1809-58442023137pt

Zac, A., Huang, Y.-C., von Moltke, A., Decker, C., & Ezrachi, A. (2025). Dark patterns and consumer vulnerability. Behavioural Public Policy, 1–50. https://doi.org/10.1017/bpp.2024.49