SciELO Preprints

Estado da publicação: O preprint não foi publicado em outro meio.

“O PRODUTO É VOCÊ”: PRIVACIDADE, EXPOSIÇÃO À PUBLICIDADE E COMPORTAMENTOS DE PROTEÇÃO ONLINE

Francisco Mateus da Silva Cruz, Ana Augusta Ferreira de Freitas, Felipe Roberto da Silva

https://doi.org/10.1590/1982-7849rac2027250416.por

Submetido em: 2026-11-18
Postado em: 2026-11-18 (versão 1)
(AAAA-MM-DD)

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

"O PRODUTO É VOCÊ": PRIVACIDADE, EXPOSIÇÃO À PUBLICIDADE E COMPORTAMENTOS DE PROTEÇÃO ONLINE

"YOU ARE THE PRODUCT": PRIVACY, EXPOSURE TO ADVERTISING, AND ONLINE PROTECTIVE BEHAVIORS

Francisco Mateus da Silva Cruz[1]
ORCID: https://orcid.org/0000-0003-2834-0632
franciscomateus722@gmail.com

Ana Augusta Ferreira de Freitas[1]
ORCID: https://orcid.org/0000-0002-2741-6968
ana.freitas@uece.br

Felipe Roberto da Silva[1]
ORCID: https://orcid.org/0000-0001-7902-4432
feliperoberto.silva@uece.br

[1] Universidade Estadual do Ceará, Fortaleza, CE, Brasil

RESUMO

Esta pesquisa investiga como a privacidade influencia o comportamento do consumidor no ambiente digital a partir de dois estudos independentes. O Estudo 1 analisa dados da pesquisa TIC Domicílios 2024 (n = 5.608) utilizando testes t para amostras independentes e ANOVAs bifatoriais (two-way). Os resultados indicam que consumidores mais sensíveis à privacidade apresentam menor diversidade de exposição à publicidade digital antes da realização de compras online, incluindo anúncios em sites e aplicativos, postagens em redes sociais, mensagens instantâneas, e-mails promocionais e vídeos. O Estudo 2 investiga os mecanismos psicológicos associados a comportamentos de proteção no ambiente digital, com base na Teoria da Motivação de Proteção, por meio de um survey (n = 330). Os resultados da regressão linear

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

múltipla mostram que a percepção de gravidade relacionada à coleta e uso de dados pessoais por empresas emerge como o principal preditor de comportamentos protetivos – como recusa de cookies e uso de bloqueadores de anúncios –, seguida pela autoeficácia e eficácia da resposta. Em conjunto, os achados indicam que preocupações com privacidade se traduzem em respostas comportamentais que podem limitar o alcance de estratégias de comunicação multicanal no comércio eletrônico. Ao investigar duas respostas independentes e paralelas — a redução da exposição à publicidade digital e a adoção de comportamentos de proteção —, o artigo amplia a compreensão do comportamento defensivo do consumidor no ecossistema de dados e oferece implicações para o desenvolvimento de práticas de marketing mais transparentes e responsáveis.

Palavras-chave: comércio eletrônico; marketing digital; mídias sociais; privacidade do consumidor; TIC Domicílios.

ABSTRACT

This research investigates how privacy influences consumer behavior in the digital environment through two independent studies. Study 1 analyzes data from the 2024 Brazilian ICT Households survey (n = 5,608) using independent-samples t-tests and two-way ANOVAs. The results indicate that more privacy-sensitive consumers exhibit a lower diversity of exposure to digital advertising prior to making online purchases, including ads on websites and apps, social media posts, instant messages, promotional emails, and videos. Study 2 examines the psychological mechanisms associated with protective behaviors in the digital environment, grounded in Protection Motivation Theory, through a survey (n = 330). Multiple linear regression results show that perceived severity regarding the collection and use of personal data by companies emerges as the main predictor of protective behaviors — such as rejecting cookies and using ad blockers — followed by self-efficacy and response efficacy. Taken together, the findings indicate that privacy concerns translate into behavioral responses that may limit the reach of multichannel communication strategies in e-commerce. By investigating two independent and parallel responses — reducing exposure to digital advertising and adopting protective behaviors — this paper broadens the understanding of defensive consumer behavior in the data ecosystem and offers implications for the development of more transparent and responsible marketing practices.

Keywords: e-commerce; digital marketing; social media; consumer privacy; ICT Households.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

1 Introdução

À semelhança da sátira distópica de George Orwell em *1984*, o panorama digital contemporâneo revela uma vigilância constante, agora mediada por interfaces amigáveis e processos algorítmicos que operam em segundo plano. Interações cotidianas aparentemente inócuas alimentam sistemas de personalização que se entrelaçam de maneira discreta à rotina dos usuários da Internet, permitindo que a coleta de informações ocorra sem alarde. Cada clique, busca, compra e até mesmo uma pausa durante a rolagem de um feed ou site podem ser monitorados por empresas de tecnologia que convertem esses rastros digitais em ativos de valor econômico (Véliz, 2021).

Empresas dominantes do setor digital ilustram bem essa lógica. O Google, por exemplo, utiliza dados de seu mecanismo de pesquisa para segmentar anúncios (Google, 2025) e a Meta monetiza as interações dos usuários em suas plataformas (Facebook for Creators, 2025). A Amazon personaliza ofertas com base no histórico de navegação dos clientes (Amazon Web Services, 2025), enquanto a Microsoft coleta dados de diagnóstico para aprimorar seus sistemas (Microsoft, 2025) – embora já tenha sido acusada de fazê-lo sem consentimento prévio (Oliveira, 2018). Não por acaso, essa estrutura de vigilância comercial sustenta um ecossistema de comunicação altamente orientado por dados, no qual diferentes formatos de conteúdo – como anúncios, postagens, vídeos e mensagens – são veiculados diariamente com o objetivo de influenciar comportamentos de consumo (Villanova et al., 2021).

Nesse contexto, a comunicação digital tornou-se um componente central das estratégias de marketing no comércio eletrônico (Grewal et al., 2022). No Brasil, sua relevância é evidenciada pelo crescimento expressivo dos investimentos em publicidade digital, que alcançaram R$ 37,9 bilhões em 2024 – um aumento de 60% em relação a 2020 (IAB Brasil & Kantar IBOPE Media, 2025). Entre estas estratégias, destaca-se a publicidade personalizada, que utiliza dados comportamentais e demográficos para direcionar mensagens específicas aos consumidores. Uma parcela significativa das vendas no comércio eletrônico já está associada a práticas de personalização baseadas em dados (Google, Instituto Esfera & Advertiser Perceptions, 2025).

A despeito do argumento de que o uso de dados granulares – i.e., informações altamente desagregadas e individualizadas sobre comportamentos, preferências e padrões de interação dos usuários em ambientes digitais – aperfeiçoa as campanhas de marketing e viabiliza experiências digitais personalizadas, cresce o debate em torno dos custos éticos e da necessidade de proteção à privacidade do consumidor (Dubé et al., 2024). Um exemplo recente

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

foi a controversa liberação do "Mapa do Instagram" no Brasil que, embora apresentado como uma ferramenta de engajamento social para visualizar a localização de amigos, gerou preocupações sobre a exposição de dados sensíveis (G1, 2026). Casos como este evidenciam que o acesso gratuito a plataformas digitais como Google e Instagram não implica ausência de custo – como se diz com frequência, “se o produto é grátis, o produto é você”.

Nesse cenário de personalização algorítmica, os indivíduos operam como agentes involuntários de sua própria vigilância (Pomfret et al., 2020), evidenciando uma relação assimétrica de poder que suscita profundas preocupações sobre o uso indevido de informações e a violação de direitos fundamentais (Aiolfi et al., 2021; Andrew & Baker, 2021; Lambillotte & Poncin, 2023). Embora marcos regulatórios como o Regulamento Geral de Proteção de Dados (RGPD) na União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil tenham emergido para mitigar essa assimetria, persistem desafios significativos relacionados à transparência e ao controle efetivo dos usuários sobre seus dados pessoais.

No campo acadêmico, a literatura sobre privacidade do consumidor tem avançado significativamente na análise das implicações dessas preocupações para o comportamento no comércio eletrônico. Entretanto, grande parte dos estudos concentra-se na intenção ou na decisão de compra online (Dinev & Hart, 2005; Fortes & Rita, 2016; Taylor et al., 2009; Anic et al., 2019; Bartol et al., 2023), enquanto os efeitos da privacidade sobre as interações que antecedem a compra permanecem relativamente pouco explorados. Essa lacuna torna-se particularmente relevante diante da crescente centralidade das estratégias de marketing orientadas por dados (Chellappa & Sin, 2005; Bleier & Eisenbeiss, 2015; Grewal et al., 2022), que ampliam atenção e engajamento por meio da personalização algorítmica (Sahni et al., 2018; Zhu & Chang, 2016; Mo et al., 2023), mas também podem intensificar preocupações com privacidade quando percebidas como intrusivas (Gironda & Korgaonkar, 2018; Aiolfi et al., 2021; Lee et al., 2022).

A transação online frequentemente envolve aceitar termos de uso, fornecer dados pessoais e interagir com sistemas de rastreamento e recomendação (Chua et al., 2021). Como as decisões de compra são influenciadas por estímulos distribuídos em múltiplos canais, torna-se relevante compreender se consumidores com preocupação com privacidade apresentam padrões distintos de exposição à comunicação digital. Nesse contexto, destaca-se a diversidade de exposição à publicidade digital antes da compra online, entendida nesta pesquisa como a variedade de estímulos comunicacionais – tais como anúncios em sites, postagens em redes sociais, mensagens instantâneas, e-mails promocionais e vídeos – que alcançam o indivíduo antes da conversão.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Contudo, compreender apenas os padrões de exposição não é suficiente. A literatura sobre o fenômeno do "paradoxo da privacidade", por exemplo, demonstra que indivíduos frequentemente expressam preocupação com o uso de seus dados pessoais, mas continuam adotando comportamentos que os expõem a riscos (Gerber et al., 2018; Gonçalves & Figueiredo, 2025; Norberg et al., 2007). Além disso, as preocupações com a privacidade podem variar conforme características sociodemográficas e padrões de uso da Internet (Sheehan, 2002; Lee et al., 2019; Chua et al., 2021; Kim et al., 2022). Essas evidências sugerem que a privacidade não influencia apenas a forma como os consumidores se inserem nos fluxos de comunicação digital, mas também a maneira como respondem aos riscos percebidos. Consequentemente, torna-se igualmente importante compreender os fatores que motivam comportamentos ativos de proteção (Boerman et al., 2021), como a recusa de cookies e o uso de bloqueadores de anúncios.

Diante dessa complexidade, este artigo propõe dois estudos metodologicamente independentes e conceitualmente coordenados que ampliam a compreensão da privacidade do consumidor para além da intenção ou decisão de compra. O Estudo 1 investiga, numa perspectiva macro, em que medida os comportamentos de preocupação com a privacidade e as características sociodemográficas dos indivíduos estão associados à diversidade de sua exposição à publicidade digital antes da compra online, propondo um proxy comportamental inédito para mensurar a variedade de estímulos comunicacionais que precedem o consumo. O Estudo 2, numa perspectiva micro, examina os fatores cognitivos associados à adoção de comportamentos ativos de proteção da privacidade, fundamentando-se na Teoria de Motivação de Proteção de Rogers (1975) para analisar como a avaliação da ameaça e a avaliação de enfrentamento se relacionam à adoção de medidas protetivas (Marikyan & Papagiannidis, 2023).

Embora não constituam etapas sequenciais de um mesmo modelo empírico, a articulação dos dois estudos é justificada pela possibilidade de apreender diferentes dimensões do repertório comportamental do consumidor, dificilmente contempladas por uma única investigação. Essa abordagem amplia a compreensão das respostas comportamentais à coleta e ao uso de dados pessoais, deslocando o foco de uma perspectiva centrada exclusivamente no resultado da compra para uma visão mais abrangente da experiência digital do consumidor. Com isso, o estudo aproxima as agendas de privacidade do consumidor, comunicação digital e comércio eletrônico, oferecendo implicações para pesquisadores, gestores e formuladores de políticas interessados em promover maior transparência, autonomia e proteção dos usuários.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

2 Referencial Teórico

2.1 Publicidade Digital e Canais de Comunicação

A comunicação digital engloba todas as formas de transmissão eletrônica de informações codificadas por meio de mídias digitais, abrangendo desde práticas tradicionais de publicidade até estratégias mais sofisticadas baseadas em dados; além de recomendações espontâneas entre consumidores (Grewal et al., 2022). Seja na comunicação um-para-um em e-mails e mensagens privadas, seja na um-para-muitos em postagens de redes sociais, as interações digitais se caracterizam por sua assincronia e natureza predominantemente textual e visual (Strauss et al., 2024).

A publicidade digital, enquanto subcampo da comunicação digital, tem passado por significativas transformações impulsionadas pelo avanço tecnológico, pela digitalização do consumo e pela emergência de canais interativos. Inicialmente, a publicidade era recebida com ceticismo pelos consumidores, sendo melhor avaliada quando percebida como informativa e útil à tomada de decisão (Shavitt et al., 1998). No entanto, com o desenvolvimento de tecnologias de rastreamento e mineração de dados, a personalização emergiu como um eixo central das estratégias contemporâneas de marketing digital.

A capacidade de recomendar produtos e serviços com base em históricos de compra, comportamento online e dados sociodemográficos potencializou a eficácia dos anúncios, permitindo que os varejistas direcionassem mensagens adequadas ao contexto, ao momento e ao perfil de cada segmento (Kim et al., 2001). No comércio eletrônico, essa vantagem é ampliada pela possibilidade de personalizar as comunicações e proporcionar uma experiência de consumo mais responsiva e sob medida (Villanova et al., 2021).

Campanhas de e-mail marketing sugerem que a personalização pode elevar a intenção de compra (Sahni et al., 2018), embora reduza o comportamento exploratório de busca por novidades (Fong, 2017). No varejo online, o uso de inteligência artificial para personalizar recomendações de serviços auxiliares demonstrou aumentos significativos na receita de longo prazo (Borenstein et al., 2023), enquanto estratégias voltadas à recuperação de abandono de carrinhos de compras virtuais mostram que lembretes personalizados podem ser eficazes quando alinhados às preferências individuais dos consumidores (Jiang & Turut, 2024).

2.2 Preocupações com a Privacidade

Apesar dos benefícios, o aumento da personalização – especialmente com o uso de dados de localização em tempo real e técnicas de rastreamento geoespacial (Banerjee, 2019) – suscita preocupações éticas e de privacidade. Embora anúncios personalizados aprimorem a experiência do usuário ao oferecer conteúdos mais relevantes, eles também provocam

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

apreensão quanto ao uso indevido de dados pessoais e à invasão de privacidade, podendo ou não reduzir a disposição para consumir online, principalmente quando os consumidores percebem que seus dados estão sendo explorados sem consentimento (Alhouti et al., 2016; Brown & Muchira, 2004).

Os benefícios da publicidade online coexistem com os riscos percebidos: enquanto a personalização aumenta a relevância e a credibilidade das mensagens (Aiolfi et al., 2021), essa também pode levar ao uso de bloqueadores de anúncios (Brinson & Britt, 2021), argumento este que precisa ser testado a partir de dados empíricos. Além disso, a experiência de usuários com anúncios em vídeo, sejam estes puláveis ou não, revela uma insatisfação generalizada em relação às plataformas digitais e preocupações éticas relacionadas à privacidade (Banerjee & Pal, 2023). Nesse contexto, consumidores que percebem maiores riscos tendem a rejeitar anúncios personalizados (Gironda & Korgaonkar, 2018; Kim et al., 2022).

Considerando que diferentes canais envolvem distintos mecanismos de coleta, tratamento e uso de dados pessoais, a literatura sugere que a percepção de intrusão pode variar conforme o canal utilizado e o tipo de dado explorado (Gironda & Korgaonkar, 2018). No entanto, não se sabe se esta rejeição diminui o número de canais de comunicação que influenciam a compra online. Nesta pesquisa, este construto é denominado "diversidade de exposição à publicidade digital antes da compra online", definida como o grau de variedade de canais de comunicação digital que precederam a realização de compras online. Podem incluir, por exemplo, propagandas exibidas em sites ou aplicativos, postagens em redes sociais, mensagens instantâneas enviadas por aplicativos, e-mails com ofertas promocionais ou vídeos disponíveis na Internet sobre produtos e serviços.

Diante da possibilidade de usos indevidos e violações de informações pessoais, a intensificação das preocupações com a privacidade consolidou-se como uma questão central no comércio eletrônico e esforços teóricos têm sido direcionados à compreensão de seus fatores antecedentes, consequências e respostas. Pesquisas iniciais indicaram as atitudes em relação ao marketing direto e o desejo de controle sobre a informação como bases para as preocupações com a privacidade, influenciando negativamente o comportamento de compra e o processo decisório dos consumidores (Phelps et al., 2001). Apesar de o fenômeno do paradoxo da privacidade demonstrar que as preocupações dos consumidores nem sempre se convertem em comportamentos coerentes (Gerber et al., 2018; Gonçalves & Figueiredo, 2025; Norberg et al., 2007), estudos indicam que a publicidade baseada em dados parece intensificar os receios relacionados à privacidade e ao uso indevido de informações pessoais (Aiolfi et al., 2021; Kim et al., 2019; Wang et al., 2023).

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Nesse sentido, a crescente implementação de tecnologias digitais e a coleta massiva de dados têm fomentado o debate sobre a personalização e a privacidade dos usuários (Lambillotte & Poncin, 2023). As preocupações com a privacidade no ambiente digital reduzem a disposição dos consumidores para fornecer informações pessoais e influenciam negativamente o comportamento de compra ao gerar atitudes desfavoráveis em relação ao comércio eletrônico (Anic et al., 2019). Outros estudos sugerem que elas reduzem a intenção de compra online (Dinev & Hart, 2005) e dificultam a adoção de inovações tecnológicas, atuando como barreiras mediadas para fatores como confiança e percepção de risco (Fortes & Rita, 2016; Miltgen et al., 2016). Nesse contexto, o presente estudo considera comportamentos de preocupação com privacidade como comportamentos associados ao controle sobre a coleta e uso de informações pessoais no ambiente digital (Castañeda et al., 2007).

Assim, é plausível hipotetizar que consumidores que manifestem comportamentos de preocupação com a privacidade adotem ações mais restritivas no comércio eletrônico. A exposição a múltiplos canais de comunicação – como sites, redes sociais, aplicativos de mensagens, e-mails e vídeos online – pode envolver diferentes formas de coleta e uso de informações pessoais para personalização e rastreamento. Por isso, espera-se que consumidores mais cautelosos limitem sua receptividade, apresentando uma menor diversidade de canais de comunicação associados às suas compras online. Com base nesse raciocínio, propõe-se a seguinte hipótese:

> **H1:** A presença de comportamentos de preocupação com privacidade está associada a uma menor diversidade de exposição à publicidade digital antes da compra online.

O uso da Internet envolve a participação ativa dos indivíduos na Web para se comunicar, acessar informações e realizar uma ampla gama de atividades online, que vão desde interações em redes sociais até compras em plataformas de e-commerce e compartilhamento de conteúdo (Blank & Groselj, 2014). Evidências sugerem que indivíduos mais engajados em atividades digitais tendem a apresentar maior propensão à realização de compras online (Bartol et al., 2023). Na presente pesquisa, a abrangência de atividades online refere-se ao nível de atividade dos indivíduos em múltiplas dimensões da vida digital – comunicacional, informacional, transacional, social e comercial – indicando o grau de diversidade das interações online realizadas (Blank & Groselj, 2014).

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Entretanto, esse maior envolvimento com o ambiente digital também implica maior exposição à coleta e ao uso de dados pessoais. À medida que os usuários realizam diferentes atividades online, deixam rastros de dados que podem ser capturados por empresas e utilizados para personalizar conteúdos e anúncios com base em interesses, preferências e comportamentos de navegação (Taylor et al., 2009; Tucker, 2014). Além disso, quanto mais os usuários utilizam serviços online e exploram as conveniências proporcionadas pelos recursos digitais, maior tende a ser sua exposição a riscos como fraudes e usos indevidos de informações pessoais, especialmente no contexto do comércio eletrônico (Blank & Lutz, 2018; Cloarec, 2020). Nesse sentido, há evidências de que a preocupação com o monitoramento das atividades digitais está associada a uma menor propensão à participação no e-commerce (Alkis & Kose, 2022).

Apesar desses avanços, a literatura ainda oferece pouca clareza sobre como o nível de atividade digital dos usuários altera a relação entre preocupações com privacidade e comportamentos relacionados às compras online. Ainda não está claro se indivíduos mais ativos na Internet – por gerarem maior volume de dados e estarem potencialmente mais expostos a práticas de coleta e uso de informações – tornam-se também mais sensíveis aos riscos de privacidade ao decidir como interagir com canais digitais no processo de compra.

Partindo da premissa de que usuários com maior abrangência de atividades online produzem mais dados e, consequentemente, estão mais expostos a mecanismos de monitoramento e personalização, argumenta-se que esses indivíduos podem apresentar maior sensibilidade às questões de privacidade ao interagir com diferentes canais de comunicação digital durante o processo de compra. Assim, quanto maior for a abrangência de atividades online do indivíduo, mais pronunciado tende a ser o impacto dos comportamentos de preocupação com a privacidade sobre a diversidade de exposição à publicidade digital antes da compra online. Com base nessa lógica, formula-se a seguinte hipótese:

> **H2:** A influência de comportamentos de preocupação com privacidade sobre a diversidade de exposição à publicidade digital antes da compra online é mais forte entre consumidores com maior abrangência de atividades online.

A renda tem sido apontada como um fator relevante no que se refere às preocupações com privacidade e à forma como os consumidores negociam compensações entre riscos e benefícios no ambiente digital. Diversos estudos sugerem que indivíduos com maior poder aquisitivo tendem a priorizar a proteção de suas informações pessoais, pois possuem mais recursos financeiros, ativos e transações digitais potencialmente expostos a riscos, o que pode

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

aumentar a percepção de perdas em caso de uso indevido de dados (Graeff & Harmon, 2002; Lee et al., 2019; O'Neil, 2001; Marwick et al., 2017). Em contraste, pessoas de menor renda tendem a demonstrar maior sensibilidade a recompensas imediatas associadas ao fornecimento de informações pessoais, como descontos ou benefícios promocionais (Graeff & Harmon, 2002; Lee et al., 2019).

Evidências empíricas também indicam que, embora a renda esteja positivamente associada à participação em compras online no contexto europeu, consumidores com rendas mais altas tendem a ser mais seletivos quanto aos canais utilizados durante esse processo, especialmente em relação a anúncios em redes sociais, o que sugere maior atenção a aspectos de privacidade e segurança no ambiente digital (Alkis & Kose, 2022). Esse comportamento sugere que, para esse grupo, preocupações com privacidade podem influenciar de forma mais intensa a maneira como os consumidores navegam entre diferentes canais de comunicação durante a jornada de compra.

Por outro lado, é importante notar que a literatura apresenta resultados divergentes. Alguns estudos não encontraram relação direta entre renda e preocupações com privacidade (Phelps, 2001), enquanto outros indicam que indivíduos com maior renda podem demonstrar maior disposição para compartilhar informações pessoais (Robinson, 2017). Ainda assim, não está claro se a renda apenas influencia a interação do consumidor com diferentes canais de comunicação antes das compras online.

Partindo do argumento de que indivíduos de maior renda percebem ter mais a perder em situações de exposição ou uso indevido de dados pessoais e, portanto, tendem a agir de maneira mais cautelosa ao interagir com estímulos de comunicação digital, espera-se que preocupações com privacidade exerçam um efeito mais pronunciado sobre a forma como esses consumidores utilizam diferentes canais durante o processo de compra online. Com base nesse raciocínio, firma-se a seguinte hipótese:

> **H3:** A influência de comportamentos de preocupação com privacidade sobre a diversidade de exposição à publicidade digital antes da compra online é mais forte entre consumidores de renda mais alta.

Outro aspecto relevante refere-se à influência do gênero na percepção de valor e na proteção de dados pessoais no ambiente digital. Evidências indicam que o gênero pode influenciar os níveis de preocupação com privacidade, que tendem a ser mais elevados entre mulheres (Bartol et al., 2023; O'Neil, 2001). Além disso, mulheres demonstram maior

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

sensibilidade à proteção de informações pessoais do que homens, independentemente do tipo de dado envolvido (Kim et al., 2022). Esses achados sugerem que homens e mulheres podem reagir de maneira distinta aos riscos associados ao compartilhamento de dados no ambiente online.

Parte da literatura também aponta que o impacto negativo das preocupações com a privacidade no uso de serviços online tende a ser mais forte entre o público feminino, indicando que as mulheres são mais propensas a agir de acordo com suas preocupações para proteger sua privacidade online (Baruh et al., 2017). Em linha com essa interpretação, estudos mostram que mulheres apresentam maior intenção de adotar funcionalidades de proteção de privacidade (Srivastava & Roychoudhury, 2021) e demonstram níveis mais elevados de consciência em relação à segurança digital quando comparadas aos homens (Pratama et al., 2022). Esses resultados sugerem que diferenças de gênero podem influenciar não apenas a percepção de risco, mas também a adoção de comportamentos protetivos no ambiente digital.

Apesar dessas evidências, ainda não está claro em que medida essas diferenças se refletem especificamente na forma como preocupações com privacidade influenciam comportamentos relacionados ao processo de compra online. Estudos anteriores tendem a examinar gênero e preocupações com privacidade de forma geral, mas há menos evidências sobre como essa relação se manifesta em decisões mais específicas, como a utilização de diferentes canais de comunicação digital durante compras online. Além disso, os resultados empíricos nem sempre são consistentes. Anic et al. (2019), por exemplo, não identificaram efeitos significativos do gênero sobre a preocupação com a privacidade no contexto da Croácia, sugerindo que tais diferenças podem variar conforme fatores contextuais e culturais.

Considerando as evidências que apontam maior sensibilidade das mulheres em relação à proteção de dados pessoais, argumenta-se que elas podem reagir de forma mais intensa às preocupações com privacidade ao decidir como interagir com diferentes canais de comunicação digital durante compras online. Assim, é plausível supor que os comportamentos de preocupação com a privacidade afetem mais fortemente a diversidade de exposição à publicidade digital antes da compra online entre mulheres do que entre homens. Em vista do exposto, apresenta-se a seguinte hipótese:

> **H4:** A influência de comportamentos de preocupação com privacidade sobre a diversidade de exposição à publicidade digital antes da compra online é mais forte entre mulheres.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Além disso, as preocupações dos indivíduos com a privacidade podem variar de forma complexa ao longo da vida (Sheehan, 2002). Evidências indicam que a preocupação com a privacidade tende a aumentar com a idade, de modo que indivíduos mais velhos geralmente demonstram níveis mais elevados de preocupação em relação ao uso e à divulgação de suas informações pessoais no ambiente digital (Alhouti, 2016; Lee et al., 2022). Esse grupo também apresenta maior probabilidade de sofrer danos online, como fraudes ou uso indevido de dados (Blank & Lutz, 2018), o que contribui para a intensificação da percepção de risco associada ao compartilhamento de informações pessoais ao longo do ciclo de vida (Robinson, 2017; Schomakers et al., 2019).

Entretanto, a literatura também sugere que a relação entre idade, preocupação com privacidade e comportamento digital não é linear. A percepção e a gestão da privacidade online variam significativamente entre diferentes faixas etárias. Adultos de meia-idade, por exemplo, tendem a apresentar maior percepção de risco e visões mais negativas sobre o tema quando comparados aos mais jovens, mas essa apreensão nem sempre se traduz em ações concretas de proteção, tornando-os menos proativos no uso de ferramentas de privacidade (Miltgen & Peyrat-Guillard, 2014; Van den Broeck et al., 2015).

Em contraste, usuários mais jovens, embora demonstrem níveis menores de preocupação, costumam transformar essa preocupação em comportamentos práticos de proteção. Sua maior familiaridade com o ambiente digital favorece a adoção de estratégias ativas de gestão da privacidade, fazendo com que se sintam mais responsáveis e confiantes na prevenção do uso indevido de dados (Miltgen & Peyrat-Guillard, 2014). Já entre indivíduos mais velhos, a preocupação com a privacidade tende a se manifestar principalmente por meio de maior cautela ou restrição na divulgação de informações, evidenciada por uma correlação negativa entre o nível de preocupação e a disposição para compartilhar dados pessoais (Masur, 2023).

Apesar dessas evidências, ainda não está claro como as diferenças etárias influenciam especificamente a forma como as preocupações com privacidade afetam comportamentos relacionados ao processo de compra online. Em particular, permanece pouco explorado se a maior percepção de risco observada entre consumidores mais velhos intensifica o impacto das preocupações com privacidade sobre a forma como esses indivíduos interagem com diferentes canais de comunicação digital ao realizar compras online.

Partindo da premissa de que consumidores mais velhos tendem a perceber maiores riscos associados ao compartilhamento de informações pessoais, espera-se que o efeito dos comportamentos de preocupação com privacidade sobre a diversidade de exposição à

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

publicidade digital antes da compra online seja mais pronunciado entre consumidores de maior idade. Assim, formula-se a seguinte hipótese:

> **H5:** A influência de comportamentos de preocupação com privacidade sobre a diversidade de exposição à publicidade digital antes da compra online é mais forte entre consumidores mais velhos.

Em estudos relacionados à desigualdade digital, observa-se que características socioeconômicas, como o nível educacional, podem influenciar a forma como os indivíduos percebem e gerenciam riscos associados ao uso da Internet. Evidências indicam que pessoas com maior nível educacional tendem a apresentar maior capacidade de reconhecer danos online decorrentes de práticas inadequadas de gestão de dados pessoais (Blank & Lutz, 2018). Além disso, a escolaridade também influencia a percepção de sensibilidade dos dados em nível individual, de modo que indivíduos mais escolarizados tendem a considerar seus dados pessoais como mais sensíveis e, portanto, mais dignos de proteção (Schomakers et al., 2019).

Em linha com essa evidência, Sheehan (2002) observou que usuários com maior nível educacional tendem a demonstrar níveis mais elevados de preocupação com a privacidade online. Em seu estudo, os grupos mais preocupados apresentavam uma proporção mais elevada de indivíduos com pós-graduação, enquanto os menos preocupados concentravam-se entre aqueles com níveis educacionais mais baixos, como ensino médio ou graduação. De forma semelhante, pesquisas posteriores indicam que indivíduos com alta escolaridade mantêm níveis elevados de preocupação com a privacidade independentemente da idade (Lee et al., 2019) e demonstram maior sensibilidade aos riscos relacionados à exposição de dados pessoais (Lee et al., 2022).

Adicionalmente, evidências provenientes de contextos educacionais sugerem que o nível de instrução também está associado à consciência sobre segurança digital. Estudos que analisam ambientes compostos por estudantes e docentes mostram que existe uma lacuna significativa na consciência de segurança: enquanto estudantes tendem a apresentar níveis mais baixos de conhecimento e práticas de proteção digital, docentes demonstram maior atenção a medidas de segurança e proteção de dados (Pratama et al., 2022). Esses achados reforçam a ideia de que a escolaridade pode estar associada não apenas à percepção de risco, mas também à capacidade de compreender e reagir a ameaças relacionadas à privacidade.

Partindo do argumento de que consumidores com maior grau de instrução apresentam maior sensibilidade aos riscos de privacidade e maior capacidade de reconhecer potenciais

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

danos associados ao uso de dados pessoais, argumenta-se que as preocupações com privacidade podem exercer um impacto mais pronunciado sobre seus comportamentos digitais. Assim, espera-se que os comportamentos de preocupação com a privacidade influenciem mais fortemente a diversidade de exposição à publicidade digital antes da compra online entre consumidores com maior nível educacional. Com base nessa lógica, delineia-se a seguinte hipótese:

> **H6:** A influência de comportamentos de preocupação com privacidade sobre a diversidade de exposição à publicidade digital antes da compra online é mais forte entre consumidores com maior grau de instrução.

2.3 Teoria da Motivação de Proteção

Proposta por Rogers (1975), a Teoria da Motivação de Proteção (*Protection Motivation Theory – PMT*) foi originalmente desenvolvida no contexto da saúde pública, com o objetivo de compreender o que motiva indivíduos a adotarem comportamentos protetivos diante de ameaças. Seu foco recai sobre os mecanismos cognitivos que mediam a mudança atitudinal e comportamental, buscando identificar os fatores que levam uma pessoa a adotar ou não uma resposta contra a ameaça percebida (Marikyan & Papagiannidis, 2023).

A robustez da PMT permitiu sua expansão para áreas como a ciência ambiental e a segurança da informação, sendo particularmente útil para investigar a lacuna entre a preocupação e a ação efetiva, além de identificar por que usuários muitas vezes negligenciam medidas de proteção mesmo estando cientes dos riscos (Li, 2012; Marikyan & Papagiannidis, 2023). Nesse sentido, a PMT oferece uma estrutura analítica capaz de examinar se uma ameaça é percebida como relevante, bem como se o indivíduo acredita possuir recursos e capacidade para enfrentá-la adequadamente.

Ao distinguir a percepção da ameaça da percepção da capacidade de agir, a PMT possibilita compreender processos decisórios em ambientes complexos e incertos, como aqueles marcados pela coleta e uso intensivo de dados pessoais por grandes plataformas digitais (Boerman et al., 2021). Seu diferencial reside justamente na proposição de que a motivação para se proteger resulta da interação entre dois processos cognitivos paralelos e interdependentes: a Avaliação da Ameaça e a Avaliação de Enfrentamento.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

2.3.1 Avaliação da Ameaça

No primeiro estágio da PMT, denominado Avaliação da Ameaça (*Threat Appraisal*), o indivíduo analisa o perigo externo a partir de dois componentes centrais: a Gravidade Percebida e a Vulnerabilidade Percebida.

A Gravidade Percebida refere-se à crença sobre o quão séria ou prejudicial é a ameaça (Witte, 1992). De acordo com a PMT, quanto maior a percepção de gravidade, maior tende a ser a intenção de proteção (Li, 2012). No contexto digital, essa dimensão se traduz na crença de que o processamento de dados para fins de personalização representa um problema relevante (Strycharz et al., 2019), manifestando-se na preocupação com a perda de controle sobre informações pessoais e com as possíveis consequências decorrentes da disseminação desses dados por empresas (Boerman et al., 2021; Wang et al., 2025).

Estudos indicam que a gravidade percebida está diretamente associada às consequências potenciais de incidentes de privacidade. Por exemplo, em dispositivos vestíveis como smartwatches, a gravidade é informada pela percepção do dano que poderia ocorrer caso terceiros não autorizados acessassem dados sensíveis do usuário (Williams et al., 2019). Evidências empíricas apontam que a Gravidade Percebida exerce efeito positivo e significativo sobre comportamentos de proteção, de modo que quanto mais seriamente os indivíduos avaliam a coleta e o compartilhamento de seus dados, maior a probabilidade de adotarem medidas defensivas (Boerman et al., 2021). Além disso, a percepção de gravidade tem sido associada a uma maior propensão ao *opt-out* de sistemas de personalização, pois quanto mais o processamento de dados é interpretado como um problema sério, maior a probabilidade de o indivíduo desativar mecanismos de personalização e restringir o uso de suas informações (Strycharz et al., 2019).

Assim, é plausível supor que, quando o consumidor deixa de perceber a coleta de dados como inócua e passa a entendê-la como prejudicial, aumenta sua tendência a adotar comportamentos de proteção, como excluir cookies, utilizar bloqueadores de anúncios ou ajustar configurações de privacidade. Dessa forma, formula-se a seguinte hipótese:

> **H7:** Níveis mais elevados de percepção da gravidade da ameaça à privacidade online estão associados a um maior comportamento de proteção do consumidor.

Complementarmente, a Vulnerabilidade Percebida refere-se à crença do indivíduo acerca da probabilidade de vir a sofrer os efeitos de uma ameaça (Witte, 1992), bem como à avaliação do grau em que se percebe "exposto" a esse risco (Ham, 2016). No âmbito da PMT

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

clássica, a vulnerabilidade constitui um preditor teoricamente positivo da intenção de adotar comportamentos protetivos (Marikyan & Papagiannidis, 2023; Li, 2012).

Uma ameaça tende a gerar motivação protetiva apenas quando o indivíduo se percebe como potencialmente afetado por ela. No ambiente digital, essa percepção emerge quando o usuário entende que suas informações estão sendo efetivamente coletadas, monitoradas e compartilhadas, transformando um risco abstrato em uma preocupação concreta e pessoal (Boerman et al., 2021). Tal percepção está associada à sensação de perda de controle sobre os próprios dados (Cloarec, 2022) e à experiência de vigilância contínua no ecossistema digital (Wang et al., 2025).

Evidências empíricas corroboram a influência da vulnerabilidade percebida sobre comportamentos de proteção, ainda que de maneira não uniforme. Cloarec (2022) demonstrou que maiores níveis de vulnerabilidade aumentam significativamente a probabilidade de falsificação de informações em redes sociais – estratégia interpretada como forma ativa de proteção, destinada a "contaminar" ou dificultar o uso comercial dos dados coletados. De modo semelhante, Wang et al. (2025), ao identificarem diferentes perfis de usuários, apontaram o grupo dos cautelosos com privacidade como aquele que reporta os maiores níveis de vulnerabilidade percebida e, simultaneamente, as mais elevadas intenções de proteção da privacidade. Por outro lado, estudos com delineamentos experimentais e longitudinais mais robustos não encontraram relação direta e estatisticamente significativa entre vulnerabilidade percebida e determinados comportamentos específicos, como o opt-out de anúncios personalizados (Boerman et al., 2021; Strycharz et al., 2019).

Ainda assim, sob a lógica teórica da PMT, a percepção de suscetibilidade permanece elemento central da avaliação da ameaça. Assim, é plausível supor que, quanto maior a percepção de vulnerabilidade à ameaça à privacidade online, maior tende a ser o engajamento do consumidor em comportamentos de proteção. Dessa forma, propõe-se a seguinte hipótese:

> **H8:** Níveis mais elevados de percepção de vulnerabilidade à ameaça à privacidade online estão associados a um maior comportamento de proteção do consumidor.

2.3.2 Avaliação de Enfrentamento

O segundo estágio da PMT, denominado Avaliação de Enfrentamento (Coping Appraisal), desloca o foco da análise da ameaça para a viabilidade da resposta protetiva. Este processo é composto pela Autoeficácia e pela Eficácia da Resposta.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

A Autoeficácia, fundamentada nos estudos de Bandura (1977), descreve a confiança que o indivíduo possui em sua própria habilidade de executar a ação protetora, ou ainda, ao julgamento que o indivíduo faz acerca de sua própria capacidade de organizar e executar cursos de ação necessários para alcançar determinado desempenho (Li, 2012; Marikyan & Papagiannidis, 2023). Trata-se, portanto, do grau de confiança percebida em relação à habilidade de engajar-se em um comportamento específico (Wang et al., 2025).

No contexto da privacidade e da segurança digital, a Autoeficácia é adaptada para representar a crença do indivíduo em sua capacidade de proteger suas informações pessoais no ambiente online (Boerman et al., 2021; Ham, 2016). Importa destacar que o construto não se refere às competências técnicas objetivas do usuário, mas ao seu autojulgamento de competência – i.e., à confiança percebida (e não necessariamente às habilidades reais) para impedir ou limitar a coleta e o processamento de dados para fins de personalização (Strycharz et al., 2019).

Na lógica da PMT, a Autoeficácia é frequentemente apontada como um dos preditores mais robustos da intenção comportamental, pois quando o indivíduo acredita ser capaz de executar a ação protetiva, aumenta a probabilidade de engajamento (Marikyan & Papagiannidis, 2023). Por outro lado, baixos níveis de autoeficácia podem gerar sentimentos de desamparo, reduzindo o investimento de esforço na proteção (Marikyan & Papagiannidis, 2023; Wang et al., 2025).

No contexto digital, essa dinâmica se manifesta na medida em que indivíduos que se percebem capazes de compreender e utilizar mecanismos de privacidade tendem a adotar estratégias mais ativas de proteção, como evitar anúncios ou ajustar configurações de dados. Evidências empíricas corroboram essa relação: Ham (2016) identificou associação positiva entre autoeficácia e comportamentos de evitação de anúncios, enquanto Williams et al. (2019) demonstraram, em experimento com smartwatches, que intervenções voltadas ao aumento da autoeficácia elevaram significativamente o uso de recursos de privacidade, como bloqueios de tela e controle de permissões. Embora nem todos os estudos encontrem efeitos consistentes da autoeficácia sobre comportamentos específicos de proteção (Boerman et al., 2021), essa relação tende a se manter no nível geral da motivação protetiva.

Desse modo, sob a perspectiva teórica da PMT, a crença na própria capacidade de agir constitui elemento central da avaliação de enfrentamento e tende, em termos gerais, a favorecer o engajamento em comportamentos protetivos. Assim, formula-se a seguinte hipótese:

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

H9: Níveis mais elevados de autoeficácia estão associados a um maior comportamento de proteção do consumidor.

Já a Eficácia da Resposta refere-se à crença de que a ação protetiva adotada será efetivamente bem-sucedida em neutralizar ou mitigar a ameaça (Witte, 1992). Em termos conceituais, trata-se da avaliação que o indivíduo faz acerca da efetividade objetiva do comportamento recomendado – *i.e.*, o julgamento de que determinada resposta é capaz de reduzir o risco percebido (Marikyan & Papagiannidis, 2023). Diferentemente da Autoeficácia – que diz respeito à confiança nas próprias habilidades para executar a ação –, a Eficácia da Resposta concentra-se na confiança na ferramenta ou medida de proteção em si (Boerman et al., 2021). Essa distinção é central na PMT: mesmo que o indivíduo se perceba capaz de agir, dificilmente adotará o comportamento se não acreditar que ele produz resultados concretos (Strycharz et al., 2019).

No contexto digital, a Eficácia da Resposta corresponde à crença de que comportamentos como excluir cookies, utilizar navegação privada ou ajustar configurações de privacidade são meios eficazes de limitar a coleta e o compartilhamento de dados pessoais (Boerman et al., 2021). Assim, envolve a avaliação cognitiva dos mecanismos de enfrentamento disponíveis e o julgamento sobre o quão eficazes são tais proteções (Mousavi et al., 2020).

As evidências empíricas sugerem que a Eficácia da Resposta tende a exercer papel particularmente relevante na formação da motivação protetiva. Strycharz et al. (2019) identificaram esse construto como o preditor mais forte tanto da motivação quanto do comportamento real de opt-out, demonstrando que a crença na efetividade da desativação de personalização influenciou positivamente a decisão efetiva dos usuários, mensurada por rastreamento online.

De maneira consistente, Boerman et al. (2021) constataram que quanto maior a crença na eficácia de comportamentos como excluir cookies, maior a probabilidade de sua adoção. Adicionalmente, Wang et al. (2025), ao analisar perfis latentes de usuários, verificaram que o grupo *Privacy-Cautious* – aquele com maior intenção de proteção – apresentou os níveis mais elevados de eficácia da resposta, engajando-se em comportamentos protetivos por acreditarem que os mecanismos disponíveis eram efetivos.

Dessa forma, à luz da PMT, é plausível supor que o consumidor somente se engaja de maneira consistente em comportamentos de proteção quando acredita que tais ações são

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

capazes de produzir resultados concretos na mitigação do risco percebido. Assim, propõe-se a seguinte hipótese:

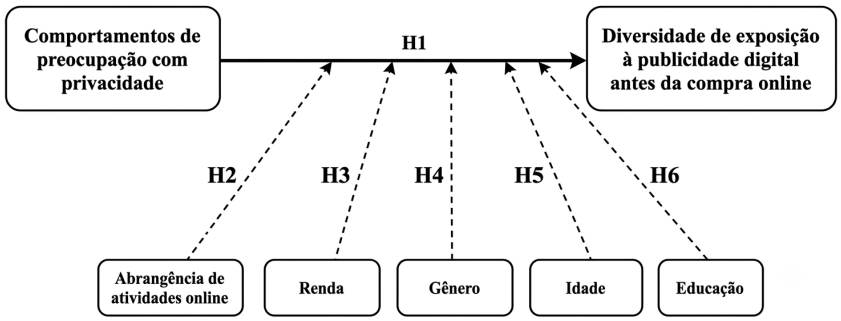
> **H10:** Níveis mais elevados de eficácia da resposta estão associados a um maior comportamento de proteção do consumidor.

3 Metodologia

3.1 Estudo 1

O Estudo 1 baseia-se em dados secundários provenientes da edição 2024 da Pesquisa TIC Domicílios (Núcleo de Informação e Coordenação do Ponto BR, 2024). Para a análise das variáveis, foram utilizados dados extraídos das seções de informações domiciliares e pessoais do questionário da referida pesquisa, além dos módulos específicos sobre uso da Internet (módulo C), comércio eletrônico (módulo H) e habilidades digitais (módulo I). A representação gráfica do arranjo metodológico e das interações entre as variáveis analisadas pode ser observada no modelo conceitual apresentado na Figura 1 a seguir:

Figura 1. *Modelo conceitual e hipóteses do Estudo 1*



A variável "diversidade de exposição à publicidade digital antes da compra online" corresponde ao grau de diversidade de canais de comunicação digital utilizados que precederam a realização de compras online. Sua construção baseou-se em cinco perguntas da TIC Domicílios, que investigam se, nos últimos 12 meses, o respondente comprou ou encomendou pela Internet após: (1) ver propagandas em sites ou aplicativos; (2) ver posts em redes sociais (Facebook, Instagram, TikTok); (3) receber mensagens via WhatsApp, Skype ou Telegram; (4) receber e-mails com ofertas; e (5) ver vídeos na Internet sobre produtos/serviços. Cada item apresenta as opções de resposta "Sim", "Não", "Não sabe", "Não respondeu" e "Não

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

se aplica", sendo estas três últimas tratadas como valores ausentes. A partir dos cinco itens, foi construído um escore variando de 0 a 5, obtido pela soma das respostas afirmativas.

A variável "comportamentos de preocupação com privacidade" foi operacionalizada a partir de três indicadores extraídos da pesquisa TIC Domicílios. A seleção desses itens foi orientada com base nas duas dimensões teóricas propostas por Castañeda e Montoro (2007) e Castañeda et al. (2007) – controle sobre a coleta e controle sobre o uso de informações pessoais no ambiente digital –, que fundamentam conceitualmente a estrutura da variável. Os três indicadores que compõem a variável foram selecionados com base em comportamentos distintos, porém complementares, relacionados à preocupação com a privacidade no ambiente digital. O primeiro verifica se o respondente deixou de usar a Internet nos últimos 12 meses por preocupações com segurança ou privacidade, refletindo uma percepção de risco generalizada. O segundo investiga se o indivíduo evitou realizar compras online no mesmo período por receio de fornecer informações pessoais, evidenciando uma hesitação associada ao controle sobre a coleta de dados. Já o terceiro avalia se, nos últimos três meses, o respondente alterou configurações de privacidade em dispositivos, contas ou aplicativos com o intuito de restringir o compartilhamento de dados pessoais, comportamento que expressa uma ação de controle sobre o uso dessas informações e limitar sua exposição ou reutilização por terceiros. Cada indicador apresenta respostas binárias ("Sim"; "Não").

Para fins analíticos, foi criada uma variável dummy que identifica se o indivíduo demonstrou alguma preocupação com a privacidade. Indivíduos que responderam "Sim" a pelo menos um dos três indicadores foram classificados no grupo "com preocupação com a privacidade", enquanto aqueles que responderam "Não" a todos os itens foram alocados no grupo "sem preocupação com a privacidade". Essa classificação permitiu comparar dois perfis distintos de consumidores, considerando-se conjuntamente as dimensões de coleta e uso de informações pessoais.

A variável "abrangência de atividades online" buscou captar o nível de atividade dos indivíduos em múltiplas dimensões da vida digital: comunicacional, informacional, transacional, social e comercial. Para mensurá-la, foi criada uma variável composta que agregou diferentes categorias de uso da Internet ao longo dos últimos três a doze meses anteriores à pesquisa, indicando o grau de diversidade das interações online realizadas (Blank & Groselj, 2014). Foram consideradas atividades equivalentes às empregadas no estudo de Bartol et al. (2023), incluindo: (1) envio e recebimento de e-mails; (2) envio de mensagens instantâneas por plataformas como Facebook, Skype ou WhatsApp; (3) chamadas de voz ou vídeo por programas como Skype ou WhatsApp; (4) busca por informações sobre produtos e

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

serviços; (5) busca por informações relacionadas à saúde; (6) realização de consultas bancárias, pagamentos ou transações financeiras; (7) leitura de jornais, revistas ou notícias online; (8) compartilhamento de conteúdo como textos, imagens, vídeos ou músicas; (9) streaming de música por plataformas como Spotify, Deezer ou YouTube; e (10) venda ou anúncio de produtos ou serviços na Internet. Cada indicador apresenta respostas binárias ("Sim"; "Não"). Para cada resposta afirmativa, foi atribuído um ponto, compondo um escore de atividade digital com variação de 0 a 10.

Para fins analíticos, o escore de atividade digital foi posteriormente categorizado em três grupos: grupo 1 (baixa atividade digital), com escores de 0 a 5; grupo 2 (atividade digital moderada), com escores de 6 a 8; e grupo 3 (alta atividade digital), com escores de 9 a 10. Optou-se pelo uso da mediana como critério de categorização, visto que o escore não apresentou distribuição normal, característica comum em variáveis discretas desse tipo, nas quais há maior concentração de respondentes em determinados intervalos.

Foram incluídas variáveis demográficas como moderadoras na análise. A renda foi recodificada a partir da variável original em três estratos simplificados, com base no salário-mínimo vigente em 2024 (R$ 1.412,00). A mediana da amostra foi usada como referência para ajustar os cortes e equilibrar o tamanho dos grupos. Por sua vez, a variável gênero foi considerada em formato binário, com as categorias masculino e feminino. Já a idade foi codificada em dois grupos: Grupo 1, formado por indivíduos com idade entre 10 e 34 anos (categorias 1 a 3), e Grupo 2, composto por respondentes com 35 anos ou mais (categorias 4 a 6). Por fim, a educação organizou os participantes em quatro níveis: (1) analfabetos ou com educação infantil; (2) ensino fundamental completo; (3) ensino médio completo ou equivalente; e (4) ensino superior, incluindo graduação e pós-graduação.

O banco de dados inicial era composto por 21.170 respondentes. Foram incluídos apenas os indivíduos com 10 anos ou mais de idade. Após a aplicação dos critérios de inclusão, permaneceram 5.608 casos válidos para análise. A principal razão para essa redução foi a elevada quantidade de dados ausentes nas variáveis relacionadas ao construto "diversidade de exposição à publicidade digital antes da compra online".

A hipótese H1 foi testada por meio de um teste t para amostras independentes para verificar o efeito principal. Já as hipóteses H2 a H6 foram analisadas por meio de análises de variância bifatoriais (ANOVA two-way), com inclusão de termos de interação entre preocupações com a privacidade e as respectivas variáveis moderadoras propostas neste estudo. Todas as análises estatísticas foram conduzidas no software SPSS Statistics, adotando-se um nível de significância de 5% ($p < 0,05$).

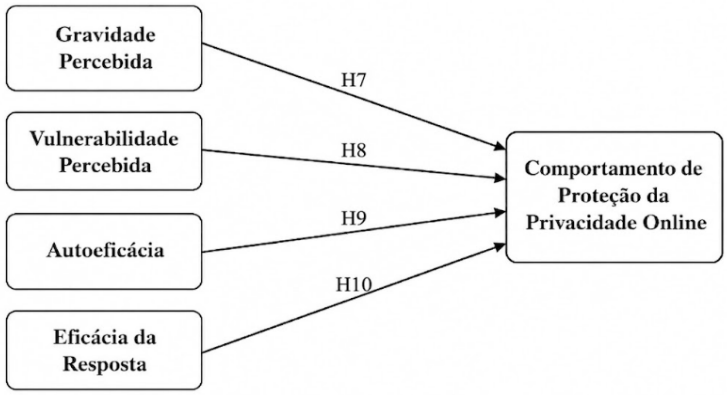
SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

3.2 Estudo 2

O Estudo 2 adotou uma abordagem quantitativa, utilizando um método de amostragem não probabilística por conveniência. A coleta de dados ocorreu entre os dias 18 e 24 de fevereiro de 2026, mediante a aplicação de um questionário estruturado via Google Forms, elaborado para mensurar os construtos da PMT (Rogers, 1975), com base nas medidas propostas por Boerman et al. (2021). Em conformidade com os princípios éticos de pesquisa, todos os participantes aceitaram o Termo de Consentimento Livre e Esclarecido antes do início da participação. A Figura 2 abaixo apresenta o modelo conceitual e as hipóteses estruturadas para esta etapa da pesquisa.

Figura 2

Modelo conceitual e hipóteses do Estudo 2



A variável "Gravidade Percebida" foi mensurada a partir do nível de concordância com as afirmações: (1) "Ter empresas coletando meu comportamento online é um problema para mim"; (2) "Ter empresas usando meu comportamento online para me mostrar anúncios é um problema para mim" e (3) "Ter empresas compartilhando meu comportamento online com outras empresas é um problema para mim". As respostas foram registradas em escala Likert de sete pontos (1 = discordo totalmente; 7 = concordo totalmente).

A variável "Vulnerabilidade Percebida" foi avaliada mediante os itens: (1) "Acredito que as empresas coletam informações sobre meu comportamento online"; (2) "Acredito que as empresas usam informações sobre meu comportamento online para me mostrar anúncios" e (3) "Acredito que as empresas compartilham informações sobre meu comportamento online com outras empresas". As respostas foram registradas em escala Likert de sete pontos (1 = discordo totalmente; 7 = concordo totalmente).

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Para avaliar a "Autoeficácia", foi perguntado o grau de concordância dos respondentes com as seguintes sentenças: (1) "Sou capaz de proteger minhas informações pessoais, como meu comportamento de navegação, na internet"; (2) "Me sinto confiante de que posso garantir minha privacidade na internet" e (3) "Posso garantir que as empresas não coletem minhas informações pessoais e meu comportamento na internet". As respostas foram registradas em escala Likert de sete pontos (1 = discordo totalmente; 7 = concordo totalmente).

A eficácia percebida da resposta foi mensurada questionando-se em que medida os respondentes acreditavam que determinados comportamentos seriam eficazes para eliminar a coleta, uso e compartilhamento de informações. Os comportamentos listados foram, conforme Boerman et al. (2021): (1) Usar um bloqueador de anúncios; (2) Excluir cookies; (3) Recusar cookies; (4) Usar o modo privado/anônimo em um navegador; (5) Excluir o histórico de navegação; (6) Usar sites ou ferramentas de preferência de anúncios (como as configurações de privacidade do Google ou redes sociais); (7) Ativar a função "Do Not Track" ("Não Rastrear") em um navegador; (8) Usar extensões de navegador (como Ghostery e uVPN); (9) Fornecer informações incorretas sobre si quando solicitado (por exemplo, um nome falso ou endereço de e-mail incorreto). As respostas foram registradas em escala Likert de sete pontos (1 = discordo totalmente; 7 = concordo totalmente).

Por fim, o comportamento de proteção foi avaliado solicitando-se aos participantes que indicassem a frequência com que realizam as seguintes ações, conforme Boerman et al. (2021): (1) Usar um bloqueador de anúncios; (2) Excluir cookies; (3) Decidir não visitar um site porque ele só é acessível com a aceitação de cookies; (4) Recusar cookies quando o site oferece essa opção; (5) Usar o modo de navegação anônima; (6) Excluir o histórico de navegação; (7) Usar sites ou ferramentas de preferência de anúncios (como as configurações de privacidade do Google ou redes sociais); (8) Usar a função "Do Not Track" ("Não Rastrear") do navegador; (9) Usar extensões de navegador (como Ghostery e uVPN) que dificultam a coleta de informações pessoais por empresas; (10) Fornecer informações incorretas sobre si quando solicitado (por exemplo, um nome falso ou endereço de e-mail incorreto). As respostas foram registradas em uma escala de frequência de seis pontos (1 = nunca; 2 = raramente; 3 = ocasionalmente; 4 = frequentemente; 5 = muito frequentemente; 6 = não sei). Para evitar distorções nas análises métricas, a opção "6 = não sei" foi tratada como dado ausente (*missing value*) e excluída dos cálculos descritivos e multivariados. Consequentemente, as estatísticas descritivas e os modelos de regressão baseiam-se estritamente no intervalo escalar de 1 a 5.

Diferentemente de uma abordagem exploratória isolada, que garante a unidimensionalidade por construção e mascara possíveis sobreposições (sobretudo entre

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Gravidade e Vulnerabilidade), a estrutura de mensuração dos cinco construtos teóricos do Estudo 2 foi avaliada conjuntamente por meio de Análise Fatorial Confirmatória (AFC). O modelo foi estimado no software JASP (versão 0.18) utilizando o estimador DWLS (*Diagonally Weighted Least Squares*) com correção robusta de erros padrão, método considerado o padrão-ouro para variáveis ordinais de escala Likert.

Os índices de ajuste global do modelo confirmatório de cinco fatores indicaram ajuste adequado aos dados empíricos: $\chi^2(340) = 798{,}488$; $p < 0{,}001$; CFI = 0,944; TLI = 0,938; RMSEA = 0,077 (IC 90%: [0,070; 0,084]); SRMR = 0,085; e GFI = 0,975. Além disso, esclarece-se que a sutil flutuação observada nos coeficientes de consistência interna das escalas em relação a versões anteriores decorreu da exclusão sistemática da opção "6 = não sei" na escala de Comportamento de Proteção, tratada estritamente como dado ausente (*missing value*). Esse procedimento depurou a variância e otimizou a precisão psicométrica das escalas sem alteração na quantidade de indicadores originais.

Considerando que todas as medidas foram obtidas por meio de autorrelato e coletadas em um único instrumento de pesquisa, avaliou-se a presença de variância de método comum (*Common Method Variance* – CMV) conforme as recomendações de Podsakoff et al. (2003). Para esse propósito, foi conduzido o teste de fator único de Harman, no qual todos os indicadores dos construtos foram submetidos conjuntamente a uma análise fatorial exploratória sem rotação. Os resultados revelaram a extração de oito fatores com autovalores superiores a 1, indicando uma estrutura multidimensional compatível com o modelo teórico proposto. Ademais, o primeiro fator respondeu por apenas 25,86% da variância total, percentual significativamente inferior ao limiar de 50% sugerido na literatura. Esses resultados fornecem evidências de que a variância de método comum não compromete substancialmente as relações observadas entre os construtos analisados.

Para garantir a adequação ao escopo do estudo, foi aplicada uma questão filtro no início do questionário: "Você comprou ou encomendou produtos ou serviços pela Internet, mesmo que o pagamento não tenha sido feito pela Internet?". Do total de 385 participações registradas, 330 respondentes confirmaram a prática de consumo online e compuseram a amostra final. O perfil demográfico da amostra (N = 330) é majoritariamente feminino (60%), com 39,4% de respondentes masculinos e 0,6% que preferiram não declarar o gênero.

No que tange à faixa etária, observa-se uma concentração na fase adulta: 84,24% dos participantes possuem entre 20 e 49 anos, com destaque para o grupo de 20 a 29 anos (31,21%). Quanto ao nível de instrução, a amostra revela um elevado perfil educacional, visto que mais de 72% possuem ensino superior completo ou pós-graduação. Economicamente, a distribuição

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

de renda é equilibrada nas faixas intermediárias, com maior concentração entre R$ 4.554,01 e R$ 7.590,00 (22,12%), seguida de perto pela faixa de R$ 7.590,01 a R$ 15.180,00 (21,21%).

Destaca-se que a exclusão da opção "6 = não sei" ocorreu no nível do item, e não do respondente. Como o comportamento de proteção foi mensurado por múltiplos itens, o escore desse construto foi calculado pela média dos itens válidos respondidos por cada participante, considerando o intervalo de 1 a 5. Esse procedimento permitiu preservar participantes que assinalaram "não sei" em um ou mais itens específicos, desde que apresentassem respostas válidas suficientes para o cálculo do escore, evitando a exclusão automática de casos inteiros em razão de dados ausentes em itens isolados. Dessa forma, os 330 respondentes da amostra filtrada foram preservados na análise de regressão linear múltipla, sem perda de observações por esse motivo.

A análise de dados foi realizada no software SPSS, adotando-se os procedimentos recomendados por Hair et al. (2009) para análises multivariadas em ciências sociais aplicadas. Inicialmente, realizou-se o teste de correlação de Pearson para avaliar o grau de associação entre as variáveis e prevenir problemas de multicolinearidade. Em seguida, foram validados os pressupostos de normalidade dos resíduos, homocedasticidade, independência dos erros e ausência de multicolinearidade. Os índices de assimetria (entre -1 e +1) e de curtose (entre -2 e +2) indicaram ausência de violações severas à normalidade univariada. O atendimento a todos os pressupostos metodológicos confirmou a adequação dos dados para a aplicação da regressão linear múltipla, garantindo a robustez dos resultados.

4 Resultados

4.1 Estudo 1

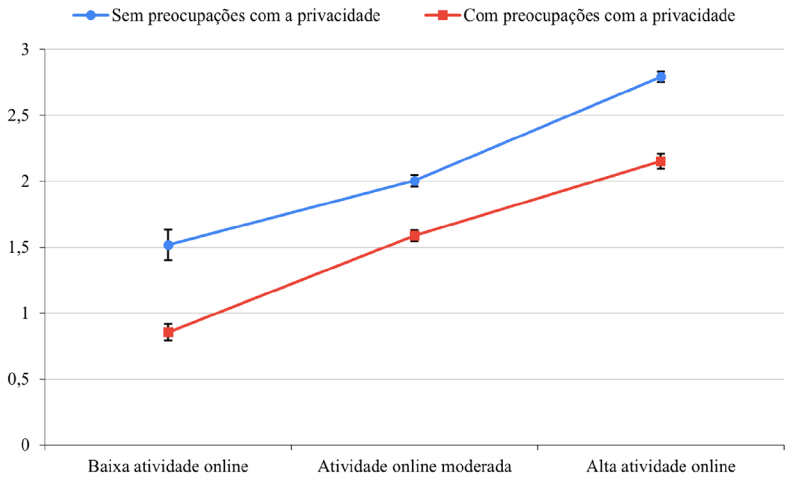
Os resultados indicaram diferença estatisticamente significativa, corroborando a hipótese H1. Consumidores que manifestaram comportamentos de preocupação com a privacidade apresentaram menor diversidade de exposição à publicidade digital antes da compra online (n = 2.674; M = 1,58; DP = 1,55) em comparação aos demais (n = 2.934; M = 2,40; DP = 1,63), com diferença de médias de 0,82 (IC95%: 0,74 – 0,90). O teste de Levene indicou desigualdade de variâncias (F = 7,039; p = 0,008), mas o teste t permaneceu robusto (t(5594,494) = 19,338; p < 0,001). Assim, confirma-se H1: as preocupações com a privacidade estão associadas a uma menor diversidade de exposição à publicidade digital. O tamanho do efeito foi moderado (d de Cohen = 0,52), indicando relevância prática da diferença observada.

Quanto à H2, observaram-se efeitos principais significativos para preocupações com privacidade (F(1,5602) = 116,465; p < 0,001; η_p^2= 0,020) e abrangência de atividades online

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

(F(2,5602) = 196,284; p < 0,001; η_p^2= 0,065), além de uma interação significativa entre as variáveis (F(2,5602) = 3,562; p = 0,028; η_p^2= 0,001). Isso indica que o efeito das preocupações com privacidade sobre a diversidade de exposição varia conforme o nível de atividade online do consumidor (Figura 3). O tamanho do efeito para o efeito principal da preocupação com a privacidade foi pequeno (η_p^2= 0,020), indicando que a privacidade explica 2,0% da variabilidade observada. Na abrangência de atividades online, o tamanho do efeito foi moderado (η_p^2= 0,065). Já para o termo da interação, o tamanho de efeito calculado foi extremamente reduzido (η_p^2= 0,001), sugerindo que, embora a moderação seja estatisticamente significante devido à elevada sensibilidade e poder estatístico proporcionados pelo tamanho amostral de nível populacional (N = 5.608), sua relevância prática imediata no nível individual é de magnitude marginal (explicando 0,13% da variância).

Figura 3. *Interação entre preocupações com a privacidade e abrangência de atividades online na diversidade de exposição à publicidade digital antes da compra online.*



As médias marginais estimadas indicam que, em todos os níveis de atividade online, consumidores com comportamentos de preocupação com privacidade apresentaram menor diversidade de exposição do que aqueles sem tais preocupações, confirmando o padrão observado em H1. Entretanto, a magnitude da diferença variou entre os grupos: -0,662 entre usuários de baixa atividade (M = 0,855 vs. 1,517), -0,416 entre os de atividade moderada (M = 1,588 vs. 2,004) e -0,640 entre os de alta atividade (M = 2,152 vs. 2,792), todas significativas (p < 0,001).

As comparações post hoc com ajuste de Bonferroni também foram significativas (p < 0,001), reforçando a robustez do padrão. Assim, a hipótese H2 é parcialmente confirmada:

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

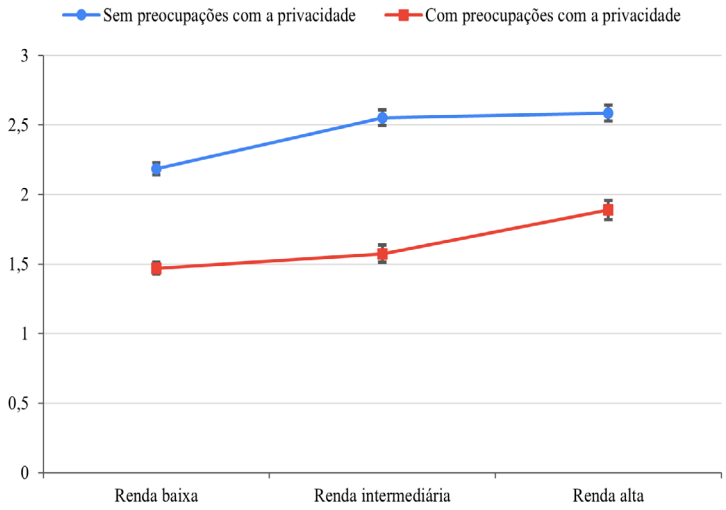
embora a maior diferença tenha ocorrido entre usuários de baixa atividade, a presença de disparidades significativas também entre usuários de alta atividade sustenta a existência de um efeito moderador. Contudo, a interação revelou um padrão mais complexo do que o previsto, já que a maior diferença ocorreu entre usuários de baixa atividade online.

Em relação à H3, a ANOVA revelou um efeito principal significativo para as preocupações com privacidade ($F(1,5415) = 308,042$; $p < 0,001$; $\eta_p^2 = 0,054$), que explica 5,4% da variabilidade. O efeito principal da renda também foi significativo ($F(2,5415) = 31,184$; $p < 0,001$; $\eta_p^2 = 0,011$), indicando que a renda explica cerca de 1,1% da variância. A interação apresentou significância estatística ($F(2,5415) = 3,881$; $p = 0,021$; $\eta_p^2 = 0,001$), oferecendo suporte à hipótese H3. Contudo, o tamanho de efeito real associado a essa interação é extremamente sutil ($\eta_p^2 = 0,0014$, ou 0,14% da variância explicada). Embora estatisticamente significante devido ao elevado poder de teste da amostra populacional (N = 5.421 casos válidos), a magnitude prática individual da moderação pela renda é reduzida, revelando-se mais como um ajuste comportamental incremental do que como um diferenciador drástico.

As médias marginais estimadas mostram que, em todos os níveis de renda, consumidores com preocupações de privacidade apresentam menor diversidade de exposição do que aqueles sem tais preocupações (Figura 4), replicando o padrão observado em H1. No entanto, a magnitude dessa diferença não foi uniforme entre os grupos: entre os consumidores de renda baixa, a média foi de 2,184 para os não preocupados e 1,470 para os preocupados (diferença = -0,713); entre os de renda média, as médias foram de 2,553 e 1,574, respectivamente (diferença = -0,979); e entre os de renda alta, de 2,585 e 1,888 (diferença = -0,696). Todas as comparações post hoc com correção de Bonferroni foram estatisticamente significativas ($p < 0,001$).

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Figura 4. *Interação entre preocupações com a privacidade e renda na diversidade de exposição à publicidade digital antes da compra online.*



Embora a hipótese H3 previsse maior influência das preocupações com privacidade entre consumidores de renda alta, os resultados indicaram que a diferença foi mais pronunciada no grupo de renda intermediária. Assim, H3 é parcialmente corroborada: há interação significativa, porém o maior efeito ocorre entre indivíduos com renda pessoal entre R$ 1.412,01 e R$ 2.824,00.

Na hipótese H4, não foi observada interação significativa entre privacidade e gênero ($F(1,5604) = 0,299$; $p = 0,585$; $\eta_p^2 = 0,00$), indicando que a relação não difere entre homens e mulheres. Ainda assim, as preocupações com privacidade influenciaram negativamente a diversidade de exposição à publicidade digital antes da compra online ($F(1,5604) = 366,126$; $p < 0,001$; $\eta_p^2 = 0,061$), com médias de 2,394 para não preocupados e 1,576 para preocupados. Observa-se que o tamanho do efeito foi moderado (6,1%). O gênero isoladamente também não apresentou efeito significativo ($F(1,5604) = 0,093$; $p = 0,761$; $\eta_p^2 = 0,00$), com médias semelhantes entre homens ($M = 1,979$) e mulheres ($M = 1,992$).

Embora a diferença entre consumidores com e sem preocupações tenha sido ligeiramente maior entre mulheres (0,842) do que entre homens (0,795), essa variação não foi estatisticamente significativa. Portanto, a influência das preocupações com privacidade sobre a diversidade de exposição à publicidade digital antes da compra online mostra-se robusta e homogênea entre os gêneros, levando à rejeição de H4.

Em relação à H5, a ANOVA bifatorial indicou efeito principal significativo das preocupações com privacidade ($F(1,5604) = 366,925$; $p < 0,001$; $\eta_p^2 = 0,061$), enquanto o efeito principal do grupo de idade não foi significativo ($F(1,5604) = 0,032$; $p = 0,859$; $\eta_p^2 = 0,000$).

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Contudo, observou-se uma interação estatisticamente significativa entre as preocupações com privacidade e o grupo de idade (F(1,5604) = 4,648; p = 0,031; η_p^2 = 0,001). O tamanho de efeito associado a esta interação, todavia, é extremamente sutil (η_p^2= 0,0008, ou 0,08% da variância explicada). Embora a interação atinja significância estatística em virtude do elevado poder de teste da amostra populacional (N = 5.608), sua magnitude prática individual é marginal, indicando que a idade atua como um moderador puramente incremental no comportamento do consumidor.

As médias marginais estimadas mostram que essa influência é mais forte entre consumidores mais velhos: entre jovens, a diferença entre preocupados e não preocupados foi de 0,734 (1,629 vs. 2,363; p < 0,001), enquanto entre os mais velhos foi de 0,920 (1,529 vs. 2,449; p < 0,001). Assim, H5 é confirmada, indicando maior impacto das preocupações com privacidade entre consumidores mais velhos.

Em relação à H6, o modelo indicou efeitos principais significativos para as preocupações com privacidade (F(1,5600) = 15,027; p < 0,001; η_p^2= 0,003) – embora com tamanho de efeito diminuto – e para o grau de instrução (F(3,5600) = 10,252; p < 0,001; η_p^2= 0,005). A interação entre as preocupações com privacidade e grau de instrução, contudo, não apresentou significância estatística (F(3,5600) = 0,742; p = 0,527; η_p^2= 0,000). Portanto, a hipótese H6 não foi suportada, demonstrando que o nível educacional do consumidor não atua como moderador na relação estudada.

Vale pontuar, sob o aspecto metodológico, que a estatística F do efeito principal de privacidade em H6 (F = 15,027) exibe uma oscilação descendente acentuada em relação aos modelos anteriores (como H4 e H5, onde se manteve em patamares próximos a 360). Essa dinâmica decorre do forte desbalanceamento na distribuição amostral da variável Grau de Instrução, a qual possui uma frequência muito reduzida na categoria “Analfabeto/Educação Infantil” (resultando em um erro padrão elevado de 0,915 nas estimativas de cruzamento). Uma vez que a ANOVA no SPSS utiliza a Soma dos Quadrados Tipo III, os efeitos principais são avaliados a partir de médias marginais não ponderadas. Assim, a imprecisão gerada pelo grupo sub-representado se propaga para o cálculo do efeito principal de privacidade, reduzindo sua estatística F. A especificação original foi mantida por retratar fielmente o perfil demográfico da amostra estudada.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

4.2 Estudo 2

Antes do teste de hipóteses por regressão linear, o modelo de mensuração do Estudo 2 foi submetido a testes rigorosos de validade convergente, confiabilidade e validade discriminante a partir dos parâmetros gerados pela AFC conjunta.

A confiabilidade e a validade convergente foram avaliadas por meio da Confiabilidade Composta (CR) e da Variância Extraída Média (AVE) (Tabela 1). Todas as escalas superaram os limites recomendados pela literatura (CR > 0,70 e AVE > 0,50; Hair et al., 2009). No caso do Comportamento de Proteção, o valor de AVE ligeiramente abaixo do limiar absoluto (0,496 ~ 0,50) é plenamente aceitável e mitigado pela elevada Confiabilidade Composta do construto (CR = 0,907).

Tabela 1. Confiabilidade e Validade Convergente das Escalas (Estudo 2)

Construto	**Cargas Fatoriais Padronizadas (λ)**	**R^2 do Item**	**AVE**	**CR**
Gravidade Percebida			**0,760**	**0,904**
Item 1 (Coleta de comportamento)	0,954	0,910		
Item 2 (Uso para anúncios)	0,865	0,747		
Item 3 (Compartilhamento de dados)	0,788	0,621		
Vulnerabilidade Percebida			**0,800**	**0,922**
Item 1 (Acredito que coletam)	0,908	0,823		
Item 2 (Acredito que usam)	0,986	0,972		
Item 3 (Acredito que compartilham)	0,777	0,603		
Autoeficácia			**0,706**	**0,877**
Item 1 (Sou capaz de proteger)	0,751	0,564		
Item 2 (Me sinto confiante)	0,971	0,943		
Item 3 (Posso garantir que não coletem)	0,782	0,610		
Eficácia da Resposta	(0,450 a 0,944)	0,202 a 0,891	**0,558**	**0,917**
Comportamento de Proteção	(0,576 a 0,835)	0,332 a 0,697	**0,496**	**0,907**

Nota: Os itens detalhados das escalas longas de Eficácia da Resposta (9 itens) e Comportamento de Proteção (10 itens) apresentaram cargas fatoriais padronizadas satisfatórias e significantes ($p < 0,001$), com os intervalos de cargas descritos entre parênteses.

Para atestar a validade discriminante, aplicou-se o Critério de Fornell-Larcker combinado à razão Heterotrait-Monotrait (HTMT) (Tabela 2), considerando a possível

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

sobreposição conceitual entre Gravidade Percebida e Vulnerabilidade Percebida. Pelo critério de Fornell-Larcker, as raízes quadradas das AVEs (dispostas na diagonal em negrito) mostraram-se superiores às correlações inter-construtos correspondentes. Adicionalmente, todas as razões HTMT (dispostas acima da diagonal) mantiveram-se abaixo do exigente limite de 0,85, confirmando estatisticamente que os respondentes diferenciaram com nitidez a gravidade das consequências do risco da sua vulnerabilidade pessoal às práticas de dados corporativos.

Tabela 2. Matriz de Validade Discriminante (Fornell-Larcker e HTMT)

Construto	1. GRA	2. VUL	3. AUT	4. EFI	5. COM
1. Gravidade (GRA)	0,872	0,125	0,085	0,141	0,571
2. Vulnerabilidade (VUL)	0,110	0,894	0,331	0,080	0,147
3. Autoeficácia (AUT)	0,072	−0,275	0,840	0,283	0,454
4. Eficácia da Resposta (EFI)	0,122	−0,017	0,243	0,747	0,348
5. Comportamento de Proteção (COM)	0,502	−0,121	0,386	0,316	0,704

Nota: Os valores na diagonal em negrito representam a raiz quadrada da AVE do construto. Os valores abaixo da diagonal representam as correlações de Pearson entre os escores médios dos construtos (N = 330). Os valores acima da diagonal representam as razões Heterotrait-Monotrait (HTMT).

Além disso, as estatísticas descritivas indicaram que o Comportamento de Proteção apresentou média de 2,85 (DP = 1,01) em uma escala de 1 a 5. Entre os construtos avaliados em escala de 1 a 7, observaram-se as seguintes médias: Gravidade (M = 4,87; DP = 1,55), Vulnerabilidade (M = 6,39; DP = 1,00), Autoeficácia (M = 3,20; DP = 1,62) e Eficácia da Resposta (M = 4,63; DP = 1,39).

Para testar as hipóteses do Estudo 2, conduziu-se uma regressão linear múltipla hierárquica em quatro blocos, tendo o Comportamento de Proteção como variável dependente. Os resultados detalhados de coeficientes, colinearidade e ajuste dos modelos estão consolidados na Tabela 3.

O Modelo 1 (inserção de Gravidade) foi significativo e explicou 25,2% da variância [$R^2 = 0,252$; R^2 ajustado = 0,250; $F(1, 328) = 110,747$, $p < 0,001$]. No Modelo 2, a adição de Autoeficácia gerou um incremento significativo de 12,3% na variância explicada [$\Delta R^2 = 0,123$; F mudança $(1, 327) = 64,419$, $p < 0,001$], totalizando um R^2 de 0,375 [$F(2, 327) = 98,290$, $p < 0,001$]. O Modelo 3 incluiu Eficácia da Resposta, promovendo nova mudança significativa de 3,2% [$\Delta R^2 = 0,032$; F mudança $(1, 326) = 17,573$, $p < 0,001$; R^2 total = 0,407; $F(3, 326) = 74,705$, $p < 0,001$].

Finalmente, o Modelo 4 (Modelo Final) adicionou a Vulnerabilidade, que apresentou um incremento marginal de 0,8%, porém estatisticamente significativo [$\Delta R^2 = 0,008$; F mudança $(1, 325) = 4,250$, $p = 0,040$]. O modelo final explicou 41,5% da variância do

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Comportamento de Proteção [$R^2 = 0,415$; R^2 ajustado = 0,408; $F(4, 325) = 57,650$, $p < 0,001$; Durbin-Watson = 1,469]. Todos os fatores apresentaram índices de colinearidade adequados (VIF < 1,2), descartando problemas de multicolinearidade no modelo final.

Tabela 3. Resultados da Regressão Linear Múltipla Hierárquica para Comportamento de Proteção

Modelo	B	EP	beta	t	p-valor	Tolerância	VIF
Modelo 1							
(Constante)	1,509	0,133		11,312	< 0,001		
Gravidade	0,275	0,026	0,502	10,524	< 0,001	1,000	1,000
Modelo 2							
(Constante)	0,986	0,138		7,126	< 0,001		
Gravidade	0,261	0,024	0,477	10,893	< 0,001	0,995	1,005
Autoeficácia	0,184	0,023	0,352	8,026	< 0,001	0,995	1,005
Modelo 3							
(Constante)	0,513	0,176		2,912	0,004		
Gravidade	0,250	0,024	0,458	10,647	< 0,001	0,983	1,017
Autoeficácia	0,161	0,023	0,308	6,999	< 0,001	0,939	1,065
Eficácia da Resposta	0,129	0,031	0,185	4,192	< 0,001	0,930	1,075
Modelo 4 (Final)							
(Constante)	1,013	0,299		3,385	0,001		
Gravidade	0,257	0,024	0,469	10,877	< 0,001	0,967	1,035
Autoeficácia	0,147	0,024	0,281	6,150	< 0,001	0,862	1,160
Eficácia da Resposta	0,132	0,031	0,189	4,291	< 0,001	0,928	1,077
Vulnerabilidade	−0,078	0,038	−0,092	−2,061	0,040	0,906	1,104

Modelo 1: $R = 0,502$; $R^2 = 0,252$; $R^2aj = 0,250$; $F(1, 328) = 110,747$, $p < 0,001$.
Modelo 2: $R = 0,613$; $R^2 = 0,375$; $R^2aj = 0,372$; $\Delta R^2 = 0,123$; $F(2, 327) = 98,290$, $p < 0,001$ (F mudança = 64,419, $p < 0,001$).
Modelo 3: $R = 0,638$; $R^2 = 0,407$; $R^2aj = 0,402$; $\Delta R^2 = 0,032$; $F(3, 326) = 74,705$, $p < 0,001$ (F mudança = 17,573, $p < 0,001$).
Modelo 4: $R = 0,644$; $R^2 = 0,415$; $R^2aj = 0,408$; $\Delta R^2 = 0,008$; $F(4, 325) = 57,650$, $p < 0,001$ (F mudança = 4,250, $p = 0,040$). Durbin-Watson = 1,469.

No que tange a Avaliação da Ameaça por parte do consumidor, a hipótese H7 previa que a percepção de gravidade da ameaça à privacidade online estaria positivamente associada ao Comportamento de Proteção. Os resultados confirmaram a relação, sendo a Gravidade o preditor mais forte do modelo ($\beta = 0,469$; $t = 10,88$; $p < 0,001$). Esse achado oferece suporte estatístico para H7, indicando que, quanto maior o dano percebido pelo usuário em relação a violações de privacidade, maior é a sua inclinação para adotar medidas protetivas.

Quanto à hipótese H8, que propunha uma relação positiva entre a Vulnerabilidade Percebida e o Comportamento de Proteção, os resultados apresentaram uma direção inesperada. Embora estatisticamente significante, o coeficiente revelou uma associação negativa ($\beta = -0,092$; $t = -2,06$; $p = 0,040$), indicando que níveis mais elevados de vulnerabilidade estão

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

associados a uma ligeira redução no comportamento de proteção. Portanto, a hipótese não foi suportada, dado que o aumento da percepção de exposição direta não se traduziu em maior comportamento de proteção.

No que tange aos mecanismos de enfrentamento, as hipóteses H9 e H10 foram plenamente corroboradas. A Autoeficácia (H9) demonstrou um impacto positivo e significativo no comportamento ($\beta = 0{,}281$; $t = 6{,}15$; $p < 0{,}001$), validando a premissa de que a confiança percebida do indivíduo em sua capacidade de proteger suas informações pessoais é fundamental para o comportamento de proteção da privacidade no contexto da compra online. Da mesma forma, a Eficácia da Resposta (H10) associou-se positivamente à variável dependente ($\beta = 0{,}189$; $t = 4{,}29$; $p < 0{,}001$). Portanto, este resultado suporta H10, corroborando a ideia de que, quando o usuário acredita que as ferramentas e ações de proteção disponíveis são de fato úteis para mitigar as ameaças, ele tende a implementá-las com maior frequência.

5 Discussão

Quanto ao Estudo 1, os resultados indicam que a presença de comportamentos de preocupação com a privacidade está associada à redução da diversidade de exposição à publicidade digital antes da compra online, com variações significativas em três dos cinco moderadores analisados. Para a segmentação de consumidores sensíveis à privacidade, fatores como idade, renda e nível de atividade online mostraram-se mais relevantes do que gênero ou escolaridade. A confirmação de H1 demonstra que, embora a comunicação digital desempenhe papel central no estímulo ao consumo, seus efeitos podem ser atenuados pela influência negativa das preocupações com a privacidade, que permanecem como uma barreira comportamental significativa no comércio eletrônico (Alhouti et al., 2016; Bartol et al., 2023; Dinev & Hart, 2005; Fortes & Rita, 2016).

Com o avanço das tecnologias de personalização, a comunicação digital no comércio eletrônico tornou-se cada vez mais ancorada em dados comportamentais, históricos de navegação e algoritmos sofisticados (Grewal et al., 2022; Villanova et al., 2021). Se, por um lado, essa sofisticação amplia o poder persuasivo das mensagens, por outro, pode intensificar percepções de intrusão (Lee et al., 2022; Gironda & Korgaonkar, 2018), especialmente entre consumidores com maior desejo de controle sobre seus dados (Taylor et al., 2009; Tucker, 2014). O resultado de H1 ilustra essa ambivalência: consumidores atentos às práticas de coleta e uso de informações tendem a adotar posturas defensivas, como ignorar anúncios e, de forma mais incisiva, evitar a efetivação de compras online mesmo diante desses estímulos. Assim como Aiolfi et al. (2021) demonstraram que a preocupação pode levar à evitação da publicidade

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

comportamental, e Baruh et al. (2017) identificaram redução no uso geral de serviços online, o presente resultado sugere que a diminuição da diversidade de exposição à publicidade digital antes da compra online constitui estratégia similar de defesa da privacidade.

De modo complementar, embora não tenham analisado estímulos específicos de comunicação digital, Anic et al. (2019) observaram que a preocupação com a privacidade não afeta diretamente a realização de compras online, mas reduz atitudes favoráveis ao e-commerce, as quais, por sua vez, elevam a propensão à compra. Nesse sentido, a menor diversidade de exposição observada neste estudo pode ser interpretada como manifestação comportamental desse mecanismo: uma ação concreta decorrente de uma atitude negativa em relação ao ambiente digital.

Quanto ao resultado de H2, uma explicação possível é que a diversidade de atividades digitais tende a associar-se a maior autoeficácia, a qual se relaciona a menores níveis de preocupação com a privacidade (Bartol et al., 2023). Assim, consumidores com baixa atividade online – e, presumivelmente, menor autoeficácia – podem perceber maior vulnerabilidade e responder às preocupações com comportamentos mais defensivos, como a redução da interação com múltiplos canais de comunicação antes da compra.

Por outro lado, a permanência de diferenças significativas entre consumidores de alta atividade online sugere um padrão possivelmente estratégico, e não meramente restritivo. Conforme indicam Alkis e Kose (2022), consumidores que adotam medidas de proteção da privacidade frequentemente relatam maior percepção de controle e confiança, o que lhes permite manter o engajamento no comércio eletrônico. Nesse contexto, a redução da diversidade de exposição à publicidade digital antes da compra online pode refletir uma estratégia seletiva de exposição, na qual consumidores mais experientes filtram riscos para continuar usufruindo dos benefícios do ambiente digital. Ainda que os mecanismos subjacentes possam diferir entre grupos, os resultados reforçam que, em uma análise multicanal, o efeito inibidor da privacidade se mantém.

Em relação a H3, a divergência entre expectativa teórica e evidência empírica pode ser analisada à luz das ambivalências da literatura sobre renda e privacidade. Entre consumidores de baixa renda, a redução da diversidade de exposição à publicidade digital é compatível com níveis mais baixos de autoeficácia digital (Bartol et al., 2023), que tornam as preocupações com a privacidade uma barreira mais impactante, gerando reação comportamental mais acentuada.

Entre consumidores de alta renda, o efeito atenuado sugere maior confiança e capacidade de gestão de riscos, alinhando-se ao padrão de seletividade pragmática descrito por

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Alkis e Kose (2022). Uma possível interpretação é que consumidores de renda intermediária combinem elevada exposição ao ambiente digital com recursos limitados de proteção, configurando um ponto crítico entre capacidade de consumo e vulnerabilidade percebida. A análise indica, portanto, que a relação entre renda e privacidade é complexa: consumidores intermediários, mais do que os de baixa ou alta renda, parecem reagir de forma mais intensa às ameaças percebidas, apresentando a reação defensiva mais expressiva (-0,979).

O resultado de H5 pode estar associado à maior familiaridade dos consumidores mais jovens com ambientes digitais e ao uso de estratégias mais ativas de proteção online (Miltgen & Peyrat-Guillard, 2014; Masur, 2023). Em contraste, consumidores mais velhos apresentaram maior diferença entre aqueles com e sem comportamentos de preocupação com a privacidade, indicando postura mais cautelosa quanto ao uso de dados pessoais no comércio eletrônico. Tal padrão pode refletir a crescente visibilidade das práticas de coleta de dados e de escândalos corporativos envolvendo segurança da informação (Robinson, 2017), além de alinhar-se a evidências de que adultos de meia-idade e idosos tendem a manifestar níveis mais elevados de preocupação com privacidade (Van den Broeck et al., 2015).

Cumpre notar que, embora a interação proposta em H2, H3 e H5 tenha se mostrado estatisticamente significante, seu tamanho de efeito foi diminuto. Essa magnitude reduzida, contudo, é metodologicamente esperada em pesquisas observacionais de campo (surveys), onde os termos de interação são naturalmente afetados por ruídos de mensuração e raramente explicam mais do que 1% da variância (McClelland & Judd, 1993; Aguinis et al., 2005). Diante da multideterminação e da extrema complexidade do comportamento de privacidade do consumidor no ambiente digital, variáveis sociodemográficas e padrões de uso geral de internet tendem a atuar como sinalizadores de efeitos sutis e incrementais. A dimensão da amostra analisada (N = 5.608) confere precisão às estimativas e sugere que, embora sutil na prática individual, o papel moderador do perfil de atividade digital, da renda e da idade constitui um padrão consistente nos dados da TIC Domicílios 2024. Por se tratar de um único levantamento transversal, a confirmação desse padrão depende de replicações em outras edições da pesquisa e em amostras independentes.

Quanto às hipóteses H4 e H6, os resultados sugerem que não há diferenças comportamentais significativas no contexto do comércio eletrônico. Observou-se apenas uma pequena diferença nas médias, com mulheres apresentando variação ligeiramente maior entre os grupos com e sem comportamentos de preocupação com privacidade, mas essa diferença não foi suficiente para sustentar um padrão comportamental distinto, ainda que permaneça parcialmente alinhada à literatura que aponta maior impacto das preocupações com privacidade

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

sobre o comportamento feminino (Baruh et al., 2017). Esses achados convergem com Anic et al. (2019), que também não identificaram interações relevantes entre preocupação com a privacidade e gênero no comércio eletrônico.

Ao contrário do observado para as variáveis de renda, idade e atividades digitais, o grau de instrução (H6) não exerceu papel moderador sobre a relação estudada. As comparações múltiplas de Bonferroni revelam que, isoladamente, os consumidores com ensino fundamental apresentaram menor diversidade de exposição à publicidade digital antes da compra ($M = 1,75$) do que aqueles com ensino médio ($M = 2,00$; $p < 0,001$) e ensino superior ($M = 2,12$; $p < 0,001$). Entretanto, a ausência de uma interação significativa indica que essa hierarquia educacional não se altera em função das preocupações de privacidade do indivíduo. Sob uma perspectiva metodológica, a rejeição de H6 indica que o elevado poder estatístico decorrente do tamanho da amostra ($N = 5.608$) não conduziu à significância de todos os termos de interação testados. Embora esse resultado não seja, por si só, evidência da veracidade das moderações observadas em H2, H3 e H5 – uma vez que o poder de cada teste depende do tamanho do efeito e do desenho de cada modelo –, ele sugere que tais moderações não decorrem meramente do tamanho amostral.

Quanto ao Estudo 2, os resultados do modelo indicam suporte empírico para três das quatro hipóteses formuladas. A Gravidade Percebida (H7) emergiu como o principal preditor do modelo, configurando-se como o gatilho cognitivo mais robusto para a adoção de comportamentos de proteção da privacidade online. Esse resultado reforça o núcleo conceitual da PMT, segundo o qual a magnitude percebida das consequências negativas constitui elemento central na ativação da motivação de proteção. No contexto da privacidade digital, quanto mais severos são percebidos os danos potenciais decorrentes de violações de dados, maior tende a ser a disposição do consumidor para agir preventivamente.

Empiricamente, o achado converge com Boerman et al. (2021), que identificaram efeito positivo da gravidade sobre comportamentos protetivos, embora com magnitude substancialmente inferior ($\beta = 0,09$). A intensidade observada no presente estudo ($\beta = 0,469$) sugere que, no ambiente de compras online, a percepção de dano assume papel particularmente mobilizador. Evidências semelhantes são reportadas por Strycharz et al. (2019), que demonstram que a percepção de que o processamento de dados constitui um problema sério aumenta a probabilidade de ações de opt-out. Esses resultados indicam que a proteção não decorre apenas da consciência da existência do risco, mas da internalização de suas consequências como substancialmente prejudiciais.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

A centralidade da gravidade também encontra respaldo nos argumentos de Ham (2017), para quem fatores negativos tendem a exercer maior peso decisório em ambientes digitais. De modo convergente, a tipologia proposta por Wang et al. (2025) identifica que consumidores com maior intenção protetiva apresentam níveis elevados de gravidade percebida, sugerindo que a avaliação das consequências adversas funciona como elemento discriminador entre perfis passivos e proativos. Assim, os resultados fortalecem a aplicabilidade da PMT ao contexto da privacidade online ao confirmarem que a percepção de dano potencial constitui o principal catalisador da ação protetiva.

Em contraste, a Vulnerabilidade Percebida (H8) apresentou associação negativa com o comportamento de proteção. Uma explicação plausível reside no "Efeito Teto" descrito por Boerman et al. (2021), segundo o qual níveis amplamente elevados de Vulnerabilidade Percebida reduzem a variabilidade do construto e sua capacidade discriminante. Adicionalmente, do ponto de vista teórico-mensurativo, a média extremamente elevada de 6,39 (em escala de 7 pontos), combinada ao coeficiente negativo obtido, sugere uma limitação operacional dos itens de vulnerabilidade. É provável que os indicadores tenham capturado crenças factuais e diagnósticas gerais sobre o funcionamento do mercado digital (isto é, a mera constatação de que as empresas coletam e tratam dados em segundo plano) em detrimento da percepção real de suscetibilidade pessoal ao dano ou sofrimento de invasão direta, que constitui o núcleo do construto de vulnerabilidade na PMT (Rogers, 1975).

Conforme discutido por Mousavi et al. (2020), quando os níveis de ameaça e rastreamento são percebidos como um fato onipresente e incontornável do ambiente, sem que o indivíduo sinta uma ameaça ativa e direcionada a si, pode ocorrer uma paralisia comportamental ou normalização do risco. Nesse cenário, a vulnerabilidade factual isolada não mobiliza ação; ao contrário, pode reforçar o "fatalismo de privacidade", quando os indivíduos sentem que não têm controle real sobre suas informações pessoais online, levando-os a desistir de qualquer esforço para se protegerem (Williams et al., 2019).

No que se refere à avaliação de enfrentamento, a Autoeficácia (H9) apresentou efeito positivo e expressivo, confirmando seu papel como mecanismo de conversão da motivação em ação. O resultado supera o efeito observado por Ham (2017) e diverge dos achados não significativos de Boerman et al. (2021), sugerindo que, no contexto de compras online, a competência digital percebida assume papel particularmente decisivo.

Por fim, a Eficácia da Resposta (H10) também exerceu influência positiva significativa, corroborando a ideia de que a crença na utilidade das medidas de proteção é fundamental para a adoção de salvaguardas comportamentais. O achado converge com evidências de Strycharz

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

et al. (2019) e Boerman et al. (2021), bem como com os achados de Mousavi et al. (2020) e Williams et al. (2019), que demonstram que a percepção de efetividade das ferramentas disponíveis transforma preocupação em ação concreta. Assim, embora a avaliação da ameaça seja necessária, a conversão da motivação em comportamento depende fortemente da crença de que há algo eficaz a ser feito. Esses achados contribuem para o refinamento da PMT no ambiente digital ao evidenciar que a ameaça precisa ser percebida como grave, mas também gerenciável, para que se converta em comportamento protetivo efetivo.

6 Considerações Finais

Os achados desta pesquisa oferecem contribuições relevantes para a compreensão da privacidade no comércio eletrônico ao analisar, de forma paralela e conceitualmente coordenada, dois desdobramentos distintos do comportamento do consumidor. O Estudo 1 mapeou, em escala nacional, um padrão defensivo no qual os comportamentos de preocupação com a privacidade se associam a uma menor diversidade de exposição à publicidade digital antes da compra. Trata-se de uma resposta de caráter reativo, na qual a sensibilidade do indivíduo à privacidade se manifesta na redução do fluxo de comunicação que o alcança. Em paralelo, o Estudo 2 examinou, sob a ótica da PMT, os fatores cognitivos associados à adoção de comportamentos ativos de proteção da privacidade online.

Do ponto de vista gerencial, as evidências indicam que as preocupações com a privacidade podem constituir uma barreira comportamental relevante no comércio eletrônico, levando o consumidor a responder defensivamente ao rastreamento e à personalização algorítmica. Esse padrão pode limitar o alcance e a eficácia de campanhas de marketing multicanal, ao reduzir a diversidade de canais de comunicação com os quais o indivíduo interage antes da compra. A pesquisa também demonstra que a adoção de comportamentos de proteção da privacidade — como bloquear anúncios, rejeitar cookies e navegar de forma anônima — está associada principalmente à percepção da gravidade dos riscos relacionados ao uso indevido de dados, à autoeficácia e à crença na utilidade dessas medidas. Na prática, empresas altamente dependentes de estratégias baseadas em dados devem considerar que percepções mais elevadas de risco podem favorecer a adoção dessas medidas de proteção, restringindo o rastreamento e, consequentemente, a possibilidade de entrega de anúncios personalizados.

Diante do crescente escrutínio público sobre práticas de coleta e uso de dados, marcas e plataformas digitais precisam reavaliar suas estratégias de comunicação e adotar abordagens mais sensíveis às preocupações dos usuários. Ignorar as respostas comportamentais associadas

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

à privacidade pode comprometer a eficácia das ações de marketing, sobretudo em contextos em que consumidores adotam ativamente ferramentas e práticas para limitar o rastreamento online. Assim, recomenda-se que as estratégias de comunicação digital combinem personalização com práticas responsáveis e transparentes de gestão de dados, fortalecendo a confiança do consumidor e ampliando sua percepção de controle sobre informações pessoais.

Nesse sentido, consumidores mais sensíveis à privacidade podem responder melhor a abordagens menos invasivas, que valorizem segurança e controle informacional. Os comportamentos de proteção investigados – como o gerenciamento e a recusa ativa de cookies – estão no cerne dos direitos de autodeterminação informativa garantidos por marcos regulatórios globais, como a LGPD e o RGPD. Ao demonstrar que a percepção de gravidade, a autoeficácia e a eficácia da resposta moldam a reação do consumidor, os resultados sinalizam aos órgãos reguladores e de defesa do consumidor que a transparência e as interfaces de consentimento não podem ser tratadas como meras formalidades técnicas. Isso exige a adoção de políticas de privacidade apresentadas de forma clara e acessível, avisos de consentimento transparentes e selos de confiança nas interfaces digitais.

Ademais, embora gênero e escolaridade não tenham apresentado influência moderadora significativa, é fundamental que os gestores adotem cautela ao utilizar as variáveis que se mostraram estatisticamente relevantes — idade, renda e abrangência de atividade digital — para fins de segmentação. Dado que os tamanhos de efeito dessas interações são bastante sutis, esses fatores devem ser interpretados estritamente como critérios complementares e incrementais, e nunca como divisores de águas isolados para decisões drásticas de marketing. Na prática, em vez de isolar grupos demográficos de forma rígida, as empresas devem usar esses perfis para calibrar e refinar de forma sutil as suas réguas de relacionamento e as suas interfaces de consentimento.

Do ponto de vista acadêmico, esta pesquisa contribui para a literatura ao conectar as agendas de privacidade do consumidor, comunicação digital e comércio eletrônico — domínios frequentemente tratados de forma isolada —, adotando uma perspectiva que evita visões reducionistas e evidencia o caráter multifacetado da autodefesa do consumidor. Esse repertório abrange desde reações de recuo na jornada de marketing (expressas pela redução da diversidade de exposição à publicidade digital no Estudo 1) até intervenções diretas de controle de dados pessoais (Estudo 2). Ao analisar esses padrões, o estudo demonstra que as preocupações com a privacidade geram manifestações pragmáticas distintas, além de inovar ao introduzir a métrica da "diversidade de exposição à publicidade digital antes da compra". Ademais, ao estender a PMT ao e-commerce, os achados consolidam a primazia de fatores cognitivos —

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

gravidade percebida da ameaça, autoeficácia e eficácia da resposta — na mobilização de barreiras digitais de proteção.

Devido às diferenças no desenho amostral, nos preditores e nos desfechos, convém salientar que os achados não configuram etapas sequenciais de um único modelo, mas sim dois padrões distintos de resposta aos riscos percebidos. Embora amostral e analiticamente independentes, sua articulação em um mesmo artigo mostra-se pertinente, uma vez que, isoladamente, nenhum estudo capturaria a amplitude do comportamento do consumidor. Juntos, no entanto, demonstram que as preocupações com a privacidade podem restringir a receptividade comunicacional no topo do funil (Estudo 1) e, concomitantemente, acionar barreiras ativas de controle informacional durante o processamento de dados (Estudo 2), evidenciando um repertório defensivo mais abrangente do consumidor no ecossistema digital.

Apesar das contribuições teóricas e práticas, algumas limitações metodológicas devem ser consideradas separadamente para cada estudo. No Estudo 1, embora a base de dados possua representatividade nacional, a análise enfrentou uma perda expressiva de casos devido à elevada incidência de dados ausentes ou não aplicáveis nas variáveis que mensuravam a diversidade de canais associados à compra online. Já no Estudo 2, a principal limitação refere-se ao perfil da amostra de conveniência obtida (N = 330), que se caracteriza por um viés de alta escolaridade (mais de 72% com ensino superior ou pós-graduação) e concentração na faixa etária adulta de 20 a 49 anos. Essa homogeneidade limita a generalização dos mecanismos cognitivos de proteção da privacidade para a população brasileira geral, que possui maior diversidade socioeconômica. Por fim, ambos os estudos se baseiam em dados autorrelatados retrospectivos, sujeitos a possíveis vieses de recordação e de desejabilidade social.

Declaração de conflito de interesse
Os autores declaram que não há conflito de interesse.

Declaração de contribuição dos autores

Francisco Mateus da Silva Cruz
conceitualização (igual), investigação (igual), metodologia (líder), validação (igual), visualização (igual), redação – rascunho original (líder), redação – revisão e edição (igual).

Ana Augusta Ferreira de Freitas
conceitualização (igual), investigação (igual), metodologia (apoio), administração do projeto (líder), supervisão (igual), validação (igual), redação – revisão e edição (igual).

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Felipe Roberto da Silva
conceitualização (igual), curadoria de dados (líder), análise formal (líder), investigação (igual), metodologia (apoio), software (líder), supervisão (igual), validação (igual), visualização (igual), redação – revisão e edição (igual).

Declaração de disponibilidade de dados da pesquisa
Todo o conjunto de dados de apoio aos resultados deste estudo foi disponibilizado em: https://cetic.br/pt/arquivos/domicilios/2024/individuos/

Declaração de uso de IA
A ferramenta de inteligência artificial **Gemini** foi utilizada para auxiliar na revisão técnico-gramatical do texto e normalização de referências.

REFERÊNCIAS

Aguinis, H., Beaty, J. C., Boik, R. J., & Pierce, C. A. (2005). Effect size and power in assessing moderating effects of categorical variables using multiple regression: a 30-year review. *Organizational Research Methods*, 8(1), 94-115.

Aiolfi, S., Bellini, S., & Pellegrini, D. (2021). Data-driven digital advertising: Benefits and risks of online behavioral advertising. *International Journal of Retail & Distribution Management, 49*(7), 1089–1110. https://doi.org/10.1108/ijrdm-10-2020-0410

Alhouti, S., Johnson, C. M., & D'Souza, G. (2016). The complex web of values: The impact on online privacy concerns and purchase behavior. *Journal of Electronic Commerce Research, 17*(1), 22. http://www.jecr.org/sites/default/files/Paper2_1.pdf

Alkis, A., & Kose, T. (2022). Privacy concerns in consumer e-commerce activities and response to social media advertising: Empirical evidence from Europe. *Computers in Human Behavior, 137*, 107412. https://doi.org/10.1016/j.chb.2022.107412

Amazon Web Services. (2025). O que é o Amazon Personalize? Recuperado em 04 de abril de 2025, de https://docs.aws.amazon.com/pt_br/personalize/latest/dg/what-is-personalize.html

Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics*, 168(3), 565–578. https://doi.org/10.1007/s10551-019-04239-z

Anic, I.-D., Škare, V., & Kursan Milaković, I. (2019). The determinants and effects of online privacy concerns in the context of e-commerce. *Electronic Commerce Research and Applications, 36*, 100868. https://doi.org/10.1016/j.elerap.2019.100868

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological review*, 84(2), 191. https://psycnet.apa.org/doi/10.1037/0033-295X.84.2.191

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Banerjee, S. (2019). Geosurveillance, location privacy, and personalization. *Journal of Public Policy & Marketing, 38*(4), 484–499. https://doi.org/10.1177/0743915619860137

Banerjee, S., & Pal, A. (2023). I hate ads but not the advertised brands: a qualitative study on Internet users' lived experiences with YouTube ads. *Internet Research*, 33(1), 39–56. https://doi.org/10.1108/intr-06-2021-0377

Bartol, J., Vehovar, V., Bosnjak, M., & Petrovčič, A. (2023). Privacy concerns and self-efficacy in e-commerce: Testing an extended APCO model in a prototypical EU country. *Electronic Commerce Research and Applications, 60*, 101289. https://doi.org/10.1016/j.elerap.2023.101289

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review: Privacy concerns meta-analysis. *Journal of Communication*, 67(1), 26–53. https://doi.org/10.1111/jcom.12276

Blank, G., & Groselj, D. (2014). Dimensions of Internet use: amount, variety, and types. *Information, communication and society*, 17(4), 417–435. https://doi.org/10.1080/1369118x.2014.889189

Blank, G., & Lutz, C. (2018). Benefits and harms from Internet use: A differentiated analysis of Great Britain. *New Media & Society, 20*(2), 618–640. https://doi.org/10.1177/1461444816667135

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2021). Exploring motivations for online privacy protection behavior: Insights from panel data. *Communication Research*, 48(7), 953-977.

Borenstein, A., Mangal, A., Perakis, G., Poninghaus, S., Singhvi, D., Skali Lami, O., & Wei Lua, J. (2023). Ancillary services in targeted advertising: From prediction to prescription. *Manufacturing & Service Operations Management, 25*(4), 1285–1303. https://doi.org/10.1287/msom.2020.0491

Brinson, N. H., & Britt, B. C. (2021). Reactance and turbulence: Examining the cognitive and affective antecedents of ad blocking. *Journal of Research in Interactive Marketing*. https://doi.org/10.1108/jrim-04-2020-0083

Brown, M., & Muchira, R. (2004). Investigating the relationship between Internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research, 5*(1), 62–70. http://www.jecr.org/sites/default/files/05_1_p06.pdf

Castañeda, J. A., & Montoro, F. J. (2007). The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research*, 7(2), 117–141. https://doi.org/10.1007/s10660-007-9000-y

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Castañeda, J. A., Montoro, F. J., & Luque, T. (2007). The dimensionality of customer privacy concern on the internet. *Online Information Review*, 31(4), 420–439. https://doi.org/10.1108/14684520710780395

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*(2–3), 181–202. https://doi.org/10.1007/s10799-005-5879-y

Chua, H. N., Ooi, J. S., & Herbland, A. (2021). The effects of different personal data categories on information privacy concern and disclosure. *Computers & Security, 110*, 102453. https://doi.org/10.1016/j.cose.2021.102453

Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. *Technological Forecasting and Social Change, 161*, 120299. https://doi.org/10.1016/j.techfore.2020.120299

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

Cohen J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Hillside, NJ: Lawrence Erlbaum Associates.

Dinev, T., & Hart, P. (2005). Internet privacy concerns and social awareness as determinants of intention to transact. *International Journal of Electronic Commerce*, 10(2), 7–29. https://doi.org/10.2753/jec1086-4415100201

Dube, J.-P. H., Bergemann, D., Demirer, M., Goldfarb, A., Johnson, G., Lambrecht, A., Lin, T., Tuchman, A., Tucker, C. E., & Lynch, J. G. (2024). The intended and unintended consequences of privacy regulation for consumer marketing: A marketing science institute report. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.4847653

Facebook for Creators. (2025). *Facebook Content Monetization.* Recuperado em 04 de abril de 2025, de https://creators.facebook.com/tools/facebook-content-monetization?locale=pt_BR

Fong, N. M. (2017). How targeting affects customer search: A field experiment. *Management Science, 63*(7), 2353–2364. https://doi.org/10.1287/mnsc.2016.2447

Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics, 22*(3), 167–176. https://doi.org/10.1016/j.iedeen.2016.04.002

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

G1 (2026, junho 11). *Instagram passa a exibir localização exata de usuários no Brasil.* https://g1.globo.com/tecnologia/noticia/2026/06/11/instagram-passa-a-exibir-localizacao-exata-de-usuarios-no-brasil-e-gera-preocupacao.ghtml

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. Computers & Security, 77, 226–261. https://doi.org/10.1016/j.cose.2018.04.002

Gironda, J. T., & Korgaonkar, P. K. (2018). ISpy? Tailored versus invasive ads and consumers' perceptions of personalized advertising. *Electronic Commerce Research and Applications, 29*, 64–77. https://doi.org/10.1016/j.elerap.2018.03.007

Gonçalves, R. B., & Figueiredo, J. C. B. de. (2025). Paradoxo da Privacidade: Revisão Integrativa da Literatura. *Revista de Administração de Empresas*, 65(2). https://doi.org/10.1590/s0034-759020250206x

Google. (2025). *Política de privacidade.* Recuperado em 04 de abril de 2025, de https://policies.google.com/privacy?hl=pt-BR#whycollect

Google, Instituto Esfera, & Advertiser Perceptions. (2025). *Publicidade personalizada no Brasil: Impacto econômico e a necessidade de um equilíbrio regulatório.* https://esferabrasil.com.br/wp-content/uploads/2025/04/Personalized-Ads-Brazil-5-1.pdf

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *The Journal of Consumer Marketing*, 19(4), 302–318. https://doi.org/10.1108/07363760210433627

Grewal, D., Herhausen, D., Ludwig, S., & Villarroel Ordenes, F. (2022). The future of digital communication research: Considering dynamics and multimodality. *Journal of Retailing*, 98(2), 224–240. https://doi.org/10.1016/j.jretai.2021.01.007

Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2009). *Análise multivariada de dados.* Bookman editora.

Ham, C. D. (2017). Exploring how consumers cope with online behavioral advertising. *International Journal of Advertising*, 36(4), 632-658. https://doi.org/10.1080/02650487.2016.1239878

IAB Brasil & Kantar IBOPE Media. (2025). *Digital AdSpend 2025.* https://iabbrasil.com.br/pesquisa-digital-adspend-2025/

Jiang, B., & Turut, O. (2024). Targeted reminder advertising: Retailers' new weapon against cart abandonment. *Journal of Business Research, 180*, 114713. https://doi.org/10.1016/j.jbusres.2024.114713

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Kim, J. W., Lee, B. H., Shaw, M. J., Chang, H.-L., & Nelson, M. (2001). Application of decision-tree induction techniques to personalized advertisements on internet storefronts. *International Journal of Electronic Commerce, 5*(3), 45–62. https://doi.org/10.1080/10864415.2001.11044215

Kim, T., Barasz, K., & John, L. K. (2019). Why am I seeing this ad? The effect of ad transparency on ad effectiveness. *The Journal of Consumer Research, 45*(5), 906–932. https://doi.org/10.1093/jcr/ucy039

Kim, W., Park, Y., Shin, J., & Jo, M. (2022). Consumer preference structure of online privacy concerns in an IoT environment. *International Journal of Market Research, 64*(5), 630–651. https://doi.org/10.1177/14707853221080067

Lambillotte, L., & Poncin, I. (2023). Customers facing companies' content personalisation attempts: paradoxical tensions, strategies and managerial insights. *Journal of Marketing Management*, 39(3–4), 213–243. https://doi.org/10.1080/0267257x.2022.2105384

Lee, H., Wong, S. F., Oh, J., & Chang, Y. (2019). Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. *Government Information Quarterly, 36*(2), 294–303. https://doi.org/10.1016/j.giq.2019.01.002

Lee, J., Kim, C., & Lee, K. C. (2022). Exploring the personalization-intrusiveness-intention framework to evaluate the effects of personalization in social media. *International Journal of Information Management, 66*, 102532. https://doi.org/10.1016/j.ijinfomgt.2022.102532

Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. Decision support systems, 54(1), 471-481. https://doi.org/10.1016/j.dss.2012.06.010

Marikyan, D., & Papagiannidis, S. (2023). Protection motivation theory: A review. TheoryHub Book: *This handbook is based on the online theory resource: TheoryHub, 78-93.*http://open.ncl.ac.uk / ISBN: 9781739604400

Marwick, A., Fontaine, C., & Boyd, D. (2017). "Nobody sees it, nobody gets mad": Social media, privacy, and personal responsibility among low-SES youth. *Social Media+ Society*, 3(2), https://doi.org/10.1177/2056305117710455

Masur, P. K. (2023). Understanding the effects of conceptual and analytical choices on 'finding' the privacy paradox: A specification curve analysis of large-scale survey data. *Information, Communication and Society*, 26(3), 584–602. https://doi.org/10.1080/1369118x.2021.1963460

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

McClelland, G. H., & Judd, C. M. (1993). Statistical difficulties of detecting interactions and moderator effects. *Psychological Bulletin*, 114(2), 376-390.

Microsoft. (2025). *Diagnóstico, feedback e privacidade no Windows.* Recuperado em 04 de abril de 2025, de https://support.microsoft.com/pt-br/windows/diagn%C3%B3stico-feedbacke-privacidade-no-windows-28808a2b-a31b-dd73-dcd3-4559a5199319

Miltgen, C. L., Henseler, J., Gelhard, C., & Popovič, A. (2016). Introducing new products that affect consumer privacy: A mediation model. *Journal of Business Research, 69*(10), 4659–4666. https://doi.org/10.1016/j.jbusres.2016.04.015

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, 23(2), 103–125. https://doi.org/10.1057/ejis.2013.17

Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. *Decision Support Systems*, 135, 113323. https://doi.org/10.1016/j.dss.2020.113323

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *The Journal of Consumer Affairs*, 41(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Núcleo de Informação e Coordenação do Ponto BR. (2024). *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: pesquisa TIC Domicílios, ano 2024.* Disponível em: https://cetic.br/pt/arquivos/domicilios/2024/domicilios/

Oliveira, J. J. (2018, 25 de abril). *MPF processa Microsoft por coleta de dados de usuário sem autorização.* Recuperado de https://valor.globo.com/empresas/noticia/2018/04/25/mpfprocessa-microsoft-por-coleta-de-dados-de-usuario-sem-autorizacao.ghtml

O'Neil, D. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review, 19*(1), 17–31. https://doi.org/10.1177/089443930101900103

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing, 15*(4), 2–17. https://doi.org/10.1002/dir.1019

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879.

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Pomfret, L., Previte, J., & Coote, L. (2020). Beyond concern: Socio-demographic and attitudinal influences on privacy and disclosure choices. *Journal of Marketing Management, 36*(5–6), 519–549. https://doi.org/10.1080/0267257x.2020.1715465

Pratama, A. R., Firmansyah, F. M., & Rahma, F. (2022). Security awareness of single sign-on account in the academic community: The roles of demographics, privacy concerns, and Big-Five personality. *PeerJ Computer Science, 8*, e918. https://doi.org/10.7717/peerj-cs.918

Robinson, C. (2017). Disclosure of personal data in e-commerce: A cross-national comparison of Estonia and the United States. *Telematics and Informatics, 34*(2), 569–582. https://doi.org/10.1016/j.tele.2016.09.006

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology*, 91 (1), 93-114.

Sahni, N. S., Wheeler, S. C., & Chintagunta, P. (2018). Personalization in email marketing: The role of noninformative advertising content. *Marketing Science, 37*(2), 236–258. https://doi.org/10.1287/mksc.2017.1066

Schomakers, E.-M., Lidynia, C., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity – insights from Germany. *International Journal of Information Management*, 46, 142–150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

Shavitt, S., Lowrey, P., & Haefner, J. (1998). Public attitudes toward advertising: More favorable than you might think. *Journal of Advertising Research, 38*(4), 7–22. https://doi.org/10.1080/00218499.1998.12466562

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society, 18*(1), 21–32. https://doi.org/10.1080/01972240252818207

Srivastava, D. K., & Roychoudhury, B. (2021). Understanding the factors that influence adoption of privacy protection features in online social networks. *Journal of Global Information Technology Management, 24*(3), 164–182. https://doi.org/10.1080/1097198x.2021.1954416

Strauss, C., Harr, M. D., & Pieper, T. M. (2024). Analyzing digital communication: a comprehensive literature review. *Management Review Quarterly*. https://doi.org/10.1007/s11301-024-00455-8

Strycharz, J., Van Noort, G., Smit, E., & Helberger, N. (2019). Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 13(2).

SciELO Preprints - Este documento é um preprint e sua situação atual está disponível em: https://doi.org/10.1590/1982-7849rac2027250416.por

Taylor, D. G., Davis, D. F., & Jillapalli, R. (2009). Privacy concern and online personalization: The moderating effects of information control and compensation. *Electronic Commerce Research, 9*(3), 203–223. https://doi.org/10.1007/s10660-009-9036-2

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research, 51*(5), 546–562. https://doi.org/10.1509/jmr.10.0355

Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society*, 1(2), 205630511561614. https://doi.org/10.1177/2056305115616149

Véliz, C. (2021). *Privacidade é poder*. Editora Contracorrente.

Villanova, D., Bodapati, A. V., Puccinelli, N. M., Tsiros, M., Goodstein, R. C., Kushwaha, T., Suri, R., Ho, H., Brandon, R., & Hatfield, C. (2021). Retailer marketing communications in the digital age: Getting the right message to the right shopper at the right time. *Journal of Retailing*, *97*(1), 116–132. https://doi.org/10.1016/j.jretai.2021.02.001

Wang, L. H., Arch, D. N., & Metzger, M. J. (2025). Not the average user: A latent profile analysis of privacy protection appraisals in targeted advertising. *New Media & Society*, https://doi.org/10.1177/14614448251393913

Wang, Z., Yuan, R., Luo, J., Liu, M. J., & Yannopoulou, N. (2023). Does personalized advertising have their best interests at heart? A quantitative study of narcissists' SNS use among Generation Z consumers. *Journal of Business Research*, 165(114070), 114070. https://doi.org/10.1016/j.jbusres.2023.114070

Williams, M., Nurse, J. R., & Creese, S. (2019). (Smart) Watch Out! encouraging privacy-protective behavior through interactive games. *International Journal of Human-Computer Studies*, 132, 121-137. https://doi.org/10.1016/j.ijhcs.2019.07.012

Witte K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, 59, 329-349.

Este preprint foi submetido sob as seguintes condições:

- Os autores declaram que os necessários Termos de Consentimento Livre e Esclarecido de participantes ou pacientes na pesquisa foram obtidos e estão descritos no manuscrito, quando aplicável.
- Os autores declaram que a elaboração do manuscrito seguiu as normas éticas de comunicação científica.
- Os autores declaram que estão cientes que são os únicos responsáveis pelo conteúdo do preprint e que o depósito no SciELO Preprints não significa nenhum compromisso de parte do SciELO, exceto sua preservação e disseminação.
- Os autores declaram que os dados, aplicativos e outros conteúdos subjacentes ao manuscrito estão referenciados.
- O manuscrito depositado está no formato PDF.
- Os autores declaram que a pesquisa que deu origem ao manuscrito seguiu as boas práticas éticas e que as necessárias aprovações de comitês de ética de pesquisa, quando aplicável, estão descritas no manuscrito.
- Os autores declaram que uma vez que um manuscrito é postado no servidor SciELO Preprints, o mesmo só poderá ser retirado mediante pedido à Secretaria Editorial do SciELO Preprints, que afixará um aviso de retratação no seu lugar.
- Os autores concordam que o manuscrito aprovado será disponibilizado sob licença Creative Commons CC-BY.
- O autor submissor declara que as contribuições de todos os autores e declaração de conflito de interesses estão incluídas de maneira explícita e em seções específicas do manuscrito.
- Os autores declaram que o manuscrito não foi depositado e/ou disponibilizado previamente em outro servidor de preprints ou publicado em um periódico.
- Caso o manuscrito esteja em processo de avaliação ou sendo preparado para publicação mas ainda não publicado por um periódico, os autores declaram que receberam autorização do periódico para realizar este depósito.
- O autor submissor declara que todos os autores do manuscrito concordam com a submissão ao SciELO Preprints.