REVISTA TÓPICOS
ISSN 2965-6672 | Qualis A2

DARK PATTERNS E A VULNERABILIDADE DO CONSUMIDOR: O DIÁLOGO ENTRE O CDC, A LGPD E O NOVO DIREITO CIVIL DIGITAL (PL 4/2025) NA ARQUITETURA DA ESCOLHA

DARK PATTERNS AND CONSUMER VULNERABILITY: THE DIALOGUE BETWEEN THE CONSUMER PROTECTION CODE, THE GENERAL DATA PROTECTION LAW, AND THE NEW DIGITAL CIVIL LAW (BILL 4/2025) IN THE ARCHITECTURE OF CHOICE

Ciências Sociais Aplicadas • 17/06/2026

REGISTRO DOI: 10.70773/revistatopicos/781742367

Jamilly Victoria de Oliveira de Abreu
Mayckerson Alexandre Franco Santos

RESUMO

O desenvolvimento do comércio eletrônico no cenário contemporâneo trouxe à tona práticas de manipulação do comportamento do consumidor através de interfaces digitais, denominadas *dark patterns* (padrões obscuros). Diante da necessidade de compreender a extensão e os limites da proteção do utilizador no mercado virtual, este trabalho delimita o seguinte problema de pesquisa: De que forma a manipulação do consentimento e da vontade do consumidor por meio de *dark patterns* no comércio eletrônico é tutelada pelo ordenamento jurídico brasileiro, considerando o diálogo entre o CDC, a LGPD e as perspetivas de atualização do Código Civil pelo Projeto de Lei nº 4/2025? O objetivo geral deste artigo é analisar se tais práticas viciam o consentimento e violam a boa-fé objetiva, sob a ótica do Código de Defesa do Consumidor, da LGPD e do Projeto de Lei n.º 4/2025. A metodologia utilizada foi a pesquisa qualitativa e documental com método dedutivo. Os resultados indicam que o design manipulativo compromete os requisitos de liberdade e informação, tornando nulo o tratamento de dados e configurando prática abusiva. Precedentes do CONAR já reconhecem essa antijuridicidade, enquanto o PL 4/2025 supre a lacuna normativa ao vedar interfaces que limitam o discernimento. Conclui-se que a proteção da dignidade do usuário exige uma abordagem integrada entre os marcos civis e consumeristas, centrada no design ético.

Palavras-chave: Padrões enganosos; Manifestação de vontade; Proteção de dados pessoais; Defesa do consumidor; Direito civil digital.

ABSTRACT

The development of e-commerce in the contemporary scenario has brought to light practices aimed at manipulating consumer

behavior through digital interfaces, known as dark patterns. In light of the need to understand the scope and limits of user protection in the virtual marketplace, this study establishes the following research problem: How is the manipulation of consumer consent and intent through dark patterns in e-commerce protected under the Brazilian legal system, considering the interaction between the Consumer Defense Code (CDC), the General Data Protection Law (LGPD), and the perspectives for updating the Civil Code through Bill No. 4/2025? The general objective of this article is to analyze whether such practices vitiate consent and violate the principle of objective good faith from the perspective of the Consumer Defense Code, the LGPD, and Bill No. 4/2025. The methodology adopted was qualitative and documentary research using the deductive method. The results indicate that manipulative design compromises the requirements of freedom and information, rendering data processing invalid and constituting an abusive practice. Precedents from CONAR have already recognized such unlawfulness, while Bill No. 4/2025 fills the regulatory gap by prohibiting interfaces that limit users' discernment. It is concluded that the protection of user dignity requires an integrated approach between civil and consumer protection frameworks, centered on ethical design.
Keywords: Deceptive patterns; Manifestation of will; Personal data protection; Consumer protection; Digital civil law.

1. INTRODUÇÃO

A expansão da economia digital consolidou um modelo de negócio fundamentado na monetização de dados pessoais, no qual as plataformas tecnológicas passaram a empregar técnicas de design de interfaces deliberadamente projetadas para manipular as decisões dos usuários, fenômeno sistematizado pela literatura

internacional sob a denominação de *dark patterns* (Brignull, 2023; Guerra; Wienskoski, 2024, p. 139). Essas técnicas, que se valem de conhecimentos de psicologia comportamental para subverter a autonomia decisória do titular de dados no momento em que ela precisa existir, colocam em xeque os requisitos de validade do consentimento, previstos no art. 5.º, XII, da Lei n.º 13.709/2018 (LGPD), e as vedações às práticas abusivas, consagradas no Código de Defesa do Consumidor (CDC).

Embora o cenário regulatório internacional aponte para uma tendência crescente de resposta normativa, da qual são expressões o *Digital Services Act* europeu (2022), o *California Privacy Rights Act* norte-americano (2020) e as diretrizes da Autoridade Central de Proteção ao Consumidor indiana (2023), a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) identificou, em seu relatório de 2022, que o Brasil não dispunha, até aquele momento, de qualquer legislação específica sobre o tema (Guerra; Wienskoski, 2024, p. 147).

Diante desse quadro, o Projeto de Lei do Senado Federal n.º 4/2025, que propõe a inserção do Livro do Direito Civil Digital no Código Civil, representa uma virada normativa ao vedar expressamente práticas que limitam o discernimento do usuário e ao proibir que interfaces digitais sejam projetadas de forma a manipular escolhas. Adota-se assim o seguinte problema de pesquisa: De que forma a manipulação do consentimento e da vontade do consumidor por meio de *dark patterns* no comércio eletrônico é tutelada pelo ordenamento jurídico brasileiro, considerando o diálogo entre o CDC, a LGPD e as perspetivas de atualização do Código Civil pelo Projeto de Lei nº 4/2025? Definindo como objetivo geral deste artigo a análise acerca da dúvida se os *dark patterns* viciam o

consentimento do titular de dados e violam a boa-fé objetiva que deve presidir as relações digitais, à luz do CDC, da LGPD e do PL 4/2025. A pesquisa é qualitativa, bibliográfica e documental, com método dedutivo, e está estruturada em três seções: a primeira examina os fundamentos teóricos da arquitetura da escolha e a taxonomia dos *dark patterns*; a segunda analisa os efeitos jurídicos dessas técnicas sobre o consentimento, a vulnerabilidade do consumidor e o diálogo entre CDC e LGPD; e a terceira examina as respostas normativas do PL 4/2025 e as consequências jurídicas do design manipulativo.

2. MATERIAIS E MÉTODO

Trata-se de pesquisa qualitativa, de natureza bibliográfica e documental. O *corpus* documental é composto por obras doutrinárias nacionais e internacionais sobre proteção de dados pessoais, direito do consumidor e economia comportamental. No plano nacional, destacam-se Bioni (2021), Doneda (2019), Marques E Miragem (2012), além das obras de referência acerca do Código de Defesa do Consumidor. No plano internacional, recorre-se a Brignull (2023), Thaler E Sunstein (2008) E Kahneman (2012). Integram, ainda, o corpus, artigos acadêmicos de referência sobre o tema, incluindo Guerra E Wienskoski (2024), Luguri E Strahilevitz (2021) E Sampaio E Jandrey (2022), bem como os trabalhos acadêmicos correlatos de Ramadas (2023), Gonzaga (2022), Andrade (2022) E Trevisol (2023). No plano normativo, foram analisadas as fontes primárias nacionais, Constituição Federal de 1988, Lei n.º 13.709/2018 (LGPD), Lei n.º 8.078/1990 (CDC), Lei n.º 10.406/2002 (Código Civil) e o Projeto de Lei do Senado Federal n.º 4/2025, bem como normas estrangeiras de referência, notadamente o Regulamento (UE) 2016/679 (GDPR) e o Regulamento (UE) 2022/2065 (Digital Services Act).

O método empregado é o dedutivo. O raciocínio parte das premissas gerais da teoria comportamental, arquitetura da escolha e economia do comportamento, para, progressivamente, aplicá-las ao exame do ordenamento jurídico brasileiro. Verifica-se, em seguida, se as técnicas identificadas como *dark patterns* subsomem-se às hipóteses normativas de invalidade do consentimento, práticas abusivas e responsabilidade civil, bem como se o Projeto de Lei n.º 4/2025 constitui resposta normativa adequada ao fenômeno.

3. RESULTADOS E DISCUSSÃO

A análise das interfaces digitais revela que as decisões dos usuários não ocorrem de forma isolada, mas dentro de ambientes arquitetados que podem tanto promover o bem-estar quanto explorar vulnerabilidades cognitivas por meio de *dark patterns*. A investigação aborda a transição do "paternalismo libertário" para o design manipulativo, identificando como técnicas como a interface enganosa e o *roach motel* comprometem os requisitos de liberdade e transparência do consentimento exigidos pela LGPD. Sob a ótica do diálogo das fontes entre o Código de Defesa do Consumidor e a legislação de proteção de dados, examina-se a hipervulnerabilidade do indivíduo na economia de vigilância e a consequente nulidade dos negócios jurídicos viciados.

O exame se estende às inovações do Projeto de Lei n.º 4/2025, que propõe a tutela da liberdade cognitiva e da integridade mental como pilares do Direito Civil Digital, alinhando o Brasil a um movimento regulatório global de repressão ao design abusivo e promoção do “Privacy by Design”.

3.1. Arquitetura da Escolha, Dark Patterns e Manipulação Cognitiva

Todos os dias, os seres humanos são confrontados com escolhas de toda natureza. No entanto, como alertam Richard Thaler, Cass Sunstein e Lucien Balz (2013), essas decisões não ocorrem no vácuo, pois são tomadas sempre dentro de um contexto ou ambiente previamente definido, que os autores nomeiam de “arquiteturas de escolha” (Trevisol, 2023, p. 13). O conceito nasce da descoberta, pela psicologia comportamental, de que as preferências das pessoas não são estáveis, mas maleáveis. Recorrentemente, os indivíduos fazem julgamentos em cenários de incerteza, confiando em regras de experiência ou “heurísticas”, processos cognitivos majoritariamente inconscientes que ignoram parte da informação para tomar decisões mais rapidamente (Trevisol, 2023, p. 14).

A teoria do *nudge*, desenvolvida por Richard Thaler e Cass Sunstein, parte precisamente desse diagnóstico. O *nudge*, traduzível como “empurrão” ou “cutucada”, é “qualquer aspecto da arquitetura de escolha capaz de alterar o comportamento das pessoas de maneira previsível, sem proibir nenhuma opção e sem modificar de forma significativa os incentivos econômicos” (Thaler; Sunstein, 2008, p. 6). Trata-se, portanto, de uma forma de intervenção que respeita a autonomia individual, denominada pelos autores de paternalismo libertário. Parte-se da premissa de que é possível e legítimo direcionar os indivíduos em sentidos que promovam o seu bem-estar sem qualquer forma de coerção (Trevisol, 2023, p. 14). O exemplo mais célebre é a inscrição automática em planos de aposentadoria. Ao transformar a adesão na opção padrão, muito mais trabalhadores passam a poupar para o futuro do que quando precisam realizar uma escolha ativa.

O poder de influência dessas arquiteturas varia, contudo, dentro de um espectro com extremos bem definidos. De um lado, encontram-se aquelas projetadas para induzir os indivíduos a melhores decisões, tal como escolheriam em condições ideais de reflexão. De outro, estão as arquiteturas concebidas para direcionar o indivíduo por meio de "fricções excessivas ou injustificadas", dificultando determinados caminhos de ação e impedindo tomadas de decisão mais deliberadas, estratégias que atuam, sobretudo, para desencorajar comportamentos que correspondem ao melhor interesse do próprio indivíduo (Trevisol, 2023, p. 16). É nesse segundo polo que se situam os *dark patterns*, mecanismos de arquitetura da escolha que, diferentemente do *nudge*, buscam promover interesses comerciais independentemente do bem-estar do usuário, mediante a exploração de suas vulnerabilidades cognitivas (Guerra; Wienskoski, 2024, p. 141).

O termo *dark pattern* foi criado em 2010 pelo designer britânico Harry Brignull, com o propósito declarado de nomear e envergonhar empresas que adotavam interfaces enganosas em seus produtos digitais (BRIGNULL, 2023). Em 2013, Brignull aprimorou a definição, passando a descrever essas interfaces como construções deliberadas, fundamentadas no conhecimento da psicologia humana e orientadas a contrariar os interesses do próprio usuário (BRIGNULL, 2023). A dificuldade de uniformidade conceitual é amplamente reconhecida pela literatura. Mathur, Mayer e Kshirsagar (2021) identificaram ao menos 13 taxonomias distintas com critérios divergentes, demonstrando a ausência de consenso sobre os elementos constitutivos do conceito. Para fins deste trabalho, adota-se a definição proposta pela Organização para a Cooperação e Desenvolvimento Econômico em seu relatório de 2022, em razão de sua maior precisão para o campo jurídico. Assim, *dark patterns* são

compreendidos como “práticas empresariais que empregam elementos de arquitetura de escolha digital, em particular em interfaces de usuário *online*, que subvertem ou prejudicam a autonomia, a tomada de decisão ou a escolha do consumidor” (OCDE, 2022, p. 19).

No contexto específico dos *banners* de solicitação de consentimento para *cookies*, mecanismo central tanto da Lei Geral de Proteção de Dados Pessoais quanto do *General Data Protection Regulation*, a literatura identifica quatro categorias de *dark patterns* de especial relevância jurídica. A primeira é a interface enganosa. Nela, o botão “Aceitar todos os *cookies*” aparece em destaque, com cor chamativa e fonte de maior dimensão, enquanto a opção “Recusar” ou “Gerenciar preferências” é apresentada em texto reduzido e sem contraste visual, dificultando a sua localização. Essa técnica opera pelo viés da disponibilidade, uma vez que aquilo que é visualmente mais saliente tende a ser percebido como a opção recomendada (Trevisol, 2023, p. 14). A segunda categoria é o roach motel, responsável por criar uma assimetria de esforço. Aceitar os *cookies* exige apenas um clique, ao passo que recusá-los demanda a navegação por diversas telas e menus aninhados. A terceira modalidade é o *confirmshamin*g, hipótese em que o botão de recusa apresenta mensagens constrangedoras, como “Não quero proteger minha privacidade” ou “Prefiro não economizar”, estratégia fundada na culpa induzida e no constrangimento emocional (Gonzaga, 2022; Andrade, 2022). A quarta categoria, mais diretamente relacionada aos requisitos da LGPD, consiste na pré-seleção. Nela, caixas de consentimento para finalidades não essenciais, como publicidade comportamental, já aparecem previamente marcadas, exigindo ação ativa do usuário para desmarcá-las. Essa técnica opera pela inércia, pois o padrão tende a

ser interpretado como a alternativa recomendada ou socialmente aceitável.

A eficácia dessas técnicas não é acidental, estando assentada em mecanismos cognitivos sistematicamente documentados pela psicologia comportamental. Amos Tversky e Daniel Kahneman (1974) alertam que a confiança excessiva nas heurísticas pode produzir desvios de julgamento "severos e sistemáticos", tornando-os previsíveis e, consequentemente, exploráveis (Tversky; Kahneman, 1974, p. 1124). Os três vieses mais relevantes para o contexto dos *dark patterns* são: a heurística da disponibilidade, segundo a qual o que é mais visível parece mais correto ou mais comum; o viés de ancoragem, em que a primeira opção apresentada funciona como referência para as demais; e a sobrecarga informacional, hipótese em que o excesso de informações paralisa a capacidade decisória e conduz à aceitação por fadiga. A dimensão empírica desse impacto é demonstrada por estudo de Nouwens et al. (2020), segundo o qual esconder a opção de recusa na interface eleva a taxa de consentimento em 22% (Nouwens et al., 2020, p. 1).

É nesse contexto que Bioni (2021) diagnostica o chamado "paradoxo da privacidade". Embora os indivíduos afirmem valorizar a proteção de seus dados pessoais, suas condutas contradizem sistematicamente esse apreço, não em razão de negligência ou indiferença, mas porque a arquitetura de escolha foi deliberadamente concebida para explorar as limitações cognitivas do usuário. Evidencia-se, assim, a dimensão estrutural do problema. Estudo realizado pela Comissão Europeia em 2022 revelou que consumidores vulneráveis, especialmente idosos e pessoas com baixa escolaridade, são condicionados por *dark patterns* em taxa 50,89% superior à observada no consumidor médio (Nouwens et al.,

2020, p. 1). A vulnerabilidade explorada, portanto, não é apenas econômica, mas também cognitiva e estrutural, imposta por interfaces projetadas por equipes especializadas em psicologia comportamental contra usuários que enfrentam essas escolhas de forma isolada, apressada e sem recursos técnicos equivalentes. Esse diagnóstico fundamenta a necessidade de uma resposta jurídica específica, questão que será examinada nas seções seguintes.

3.2. Consentimento, Vulnerabilidade e o Diálogo Entre CDC e LGPD

O consentimento é o elemento cardeal do sistema de proteção de dados pessoais instituído pela Lei Geral de Proteção de Dados Pessoais. O vocábulo aparece 35 vezes no texto legal (BIONI, 2021), e sua definição, constante do art. 5.º, XII, é precisa: "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada". O art. 8.º complementa os requisitos formais. O consentimento deve ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade (§ 1.º); cabe ao controlador o ônus da prova de sua obtenção (§ 2.º); autorizações genéricas são nulas de pleno direito (§ 4.º); e o consentimento obtido em desconformidade com as normas da LGPD é igualmente nulo (§ 6.º). O art. 9.º acrescenta que informações enganosas ou não transparentes prestadas ao titular tornam o consentimento autonomamente inválido.

A tríade "livre, informado e inequívoco" é indissociável. A ausência de qualquer um desses qualificadores invalida integralmente o ato de consentimento (Bioni, 2021; Andrade, 2022). Os *dark patterns* comprometem sistematicamente cada um desses pilares. O

consentimento livre pressupõe que o titular não esteja submetido a coação, pressão psicológica ou desvantagem indevida decorrente da recusa ao tratamento. O *confirmshaming*, ao associar a negativa a mensagens constrangedoras, e o roach motel, ao criar uma assimetria injustificada de esforço entre aceitar e recusar, violam frontalmente esse requisito. Bioni (2021) é preciso ao afirmar que o consentimento livre deve ser "despido da influência desmesurada de terceiros".

O consentimento informado exige que o titular compreenda, de forma clara e acessível, as finalidades do tratamento de dados. A interface enganosa, que oculta opções de gerenciamento de privacidade em menus de difícil acesso e emprega linguagem técnica opaca, viola diretamente o princípio da transparência previsto no art. 6.º, VI, da LGPD, além de afrontar o art. 9.º da mesma lei. Andrade (2022) demonstra que os *dark patterns* de ocultação são especificamente direcionados à obstrução desse requisito. Já o consentimento inequívoco exige manifestação afirmativa e não ambígua do titular. A pré-seleção substitui essa ação positiva pelo silêncio ou pela inércia do usuário, resultado incompatível com o art. 5.º, XII, e com o art. 8.º, § 4.º, da LGPD. O General Data Protection Regulation, em seu art. 7.º, n.º 3, é expresso ao vedar caixas previamente marcadas como forma legítima de obtenção de consentimento, parâmetro interpretativo que ilumina a compreensão da norma brasileira.

Configurada a violação de qualquer desses requisitos, o consentimento é nulo de pleno direito, por força conjunta do art. 8.º, § 6.º, da LGPD e do art. 166, incisos II e IV, do Código Civil Brasileiro, que considera nulo o negócio jurídico cujo objeto seja ilícito ou cujo motivo determinante seja ilícito. A nulidade opera retroativamente.

Todo tratamento de dados realizado a partir de consentimento viciado é ilícito; os dados coletados devem ser eliminados; e o titular possui o direito de revogar o consentimento a qualquer tempo, conforme prevê o art. 18, IX, da LGPD. Vale registrar que o *dark pattern* do tipo roach motel, quando dificulta essa revogação, configura ilícito autônomo adicional, por inviabilizar o exercício de direito expressamente assegurado pela legislação. A síntese de Gonzaga (2022, p. 64) é elucidativa: "se o consentimento foi a base legal escolhida para conferir legitimidade ao tratamento de dados pessoais, o uso de um *Dark Pattern* que interfere nos seus requisitos essenciais acarretará a ausência de lastro para realizar as operações, lançando o tratamento à ilegalidade".

A dimensão da vulnerabilidade constitui o segundo eixo desta seção. O art. 4.º, I, do Código de Defesa do Consumidor reconhece a vulnerabilidade como pressuposto absoluto da tutela consumerista. A doutrina especializada identifica diferentes dimensões dessa vulnerabilidade: técnica, decorrente do desconhecimento acerca das características do produto ou serviço; jurídica, relacionada à incapacidade de avaliar cláusulas e consequências normativas; e informacional, ligada à impossibilidade de processar adequadamente todas as informações disponíveis, sendo esta última a predominante no ambiente digital (Marques; Miragem, 2012).

Bioni (2021) avança para o conceito de hipervulnerabilidade informacional, expressão que descreve a condição estrutural do titular de dados na economia de vigilância. Trata-se de um indivíduo submetido a políticas de privacidade cuja leitura integral demandaria centenas de horas, interfaces projetadas por equipes especializadas em psicologia comportamental e uma assimetria de

poder impossível de ser superada individualmente. Ramadas (2023) complementa que essa hipervulnerabilidade é agravada quando o consumidor é idoso, apresenta limitações cognitivas ou não teve acesso à educação mínima. Dados concretos presentes na literatura ilustram essa realidade. A Amazon exigia três etapas burocráticas para o cancelamento do serviço Prime mesmo após o usuário já ter solicitado o encerramento da assinatura. O Facebook, por sua vez, demandava cinco cliques para inscrição e vinte e quatro para cancelamento (Ramadas, 2023, p. 83-84). Esses números não representam falhas acidentais de design, mas escolhas deliberadas destinadas a explorar a vulnerabilidade cognitiva do consumidor.

O direito brasileiro oferece, nesse contexto, um importante instrumento interpretativo: o diálogo das fontes. A teoria, desenvolvida por Erik Jayme e introduzida no direito nacional por Claudia Lima Marques, sustenta que normas pertencentes a um mesmo sistema jurídico devem ser aplicadas de forma harmônica, coordenada e complementar, jamais excludente (Bioni, 2021; Marques, 2011). No caso dos *dark patterns*, CDC e LGPD não competem entre si, mas se complementam.

O fundamento normativo desse diálogo encontra-se positivado no art. 45 da LGPD, que prevê expressamente a aplicação subsidiária do CDC às relações de consumo envolvendo tratamento de dados pessoais. O mesmo *dark pattern*, portanto, incorre em violação simultânea aos dois microssistemas normativos. Pelo CDC, configura prática abusiva nos termos do art. 39, IV, dispositivo que veda prevalecer-se da fraqueza ou ignorância do consumidor, podendo ainda caracterizar publicidade enganosa ou abusiva, conforme o art. 37, § 2.º. Pela LGPD, invalida o consentimento, nos termos do art. 8.º, §

6.º, e enseja responsabilidade objetiva do controlador, conforme prevê o art. 42.

A aplicação harmônica desses diplomas não apenas amplia o arsenal normativo disponível, mas potencializa sua eficácia protetiva. A presunção absoluta de vulnerabilidade prevista no CDC reforça a hipervulnerabilidade informacional descrita por Bioni (2021), enquanto a nulidade do consentimento prevista na LGPD articula-se com a nulidade das práticas abusivas disciplinadas pelo art. 51 do CDC. Sampaio e Jandrey (2022) sintetizam essa compreensão ao afirmarem que "não há dúvidas que o uso das técnicas de *Dark Patterns* consiste em uma ameaça a consumidores e titulares de dados, visto que suas características manipulativas induzem esses indivíduos a tomar decisões que interessam às empresas, e por este motivo, devem ser rigorosamente combatidos" (Sampaio; Jandrey, 2022, p. 250).

O precedente administrativo mais relevante identificado na literatura nacional confirma esse diagnóstico. Em dezembro de 2022, a Sétima Câmara do Conselho Nacional de Autorregulamentação Publicitária analisou reclamação formulada por consumidor contra a Drogaria São Paulo. O relator reconheceu que o anúncio configurava *dark pattern* ao criar uma "arquitetura de oferta digital que serviria de isca com a intenção de promover produtos diferentes", aplicando advertência agravada à empresa por decisão unânime (Ramadas, 2023, p. 28-29; Guerra; Wienskoski, 2024, p. 150). Em março de 2023, a mesma Câmara reiterou esse entendimento em reclamação envolvendo as empresas Monetizze e Umbrella Business. O relator foi explícito:

> *Ele concordou com os termos da denúncia, considerando que a conduta da anunciante como práticas conhecidas como a prática denominada dark patterns, que coagem ou manipulam os consumidores a fazerem escolhas que muitas vezes não são do seu interesse, ou podem ser enganosas. 'São ações abusivas utilizadas no desenvolvimento de atividades comerciais, relacionadas à arquitetura de decisão online e às interfaces online de navegação, que podem prejudicar a capacidade de escolha e a decisão do consumidor'. (CONAR, 2023, p. 1).*

Esses precedentes demonstram que o ordenamento jurídico brasileiro já reconhecia a antijuridicidade dos *dark patterns* antes do PL 4/2025, por meio da aplicação analógica e complementar do CDC e da LGPD. Entretanto, conforme observado por Ramadas (2023, p. 30) e Guerra e Wienskoski (2024, p. 153), a ausência de fundamento normativo específico leva a tratamentos não uniformes pelos órgãos competentes, lacuna que o PL 4/2025 se propõe a preencher.

3.3. O PL 4/2025 e a Resposta Normativa Ao Design Manipulativo

3.3.1. Autodeterminação Digital Como Direito de Personalidade: Os Fundamentos do Livro VI do Código Civil

O Projeto de Lei n.º 4/2025 propõe a inserção do Livro VI, Do Direito Civil Digital, no Código Civil brasileiro. A iniciativa parte do diagnóstico, compartilhado pela doutrina, de que os institutos clássicos do direito privado foram forjados para um mundo

analógico e mostram-se insuficientes para tutelar as novas formas de vulnerabilidade que emergem da digitalização da vida. A própria exposição de motivos do projeto registra:

> *Fica evidente que as relações e situações jurídicas digitais já fazem parte do cotidiano do brasileiro e tornaram premente o delineamento do Direito Civil Digital, como Livro autônomo do Código Civil, em face da evidente virada tecnológica do direito, de modo a agregar inúmeras interações de institutos tradicionais e de novos institutos, relações e situações jurídicas neste ambiente digital. (BRASIL, 2025, Avulso do PL 4/2025, p. 269).*

Esse diagnóstico ressoa com a evolução doutrinária da privacidade descrita por Danilo Doneda (2019). Na análise do autor, o direito à privacidade passou de uma posição negativa, o clássico right to be let alone formulado por Warren e Brandeis em 1890, para uma posição ativa, voltada à construção de uma esfera privada em que a personalidade possa se desenvolver plenamente (Doneda, 2019, p. 31). O PL 4/2025 reflete essa evolução ao estabelecer, no art. 2.027-A, que o direito civil digital visa fortalecer o exercício da autonomia privada e preservar a dignidade das pessoas no ambiente digital.

Os fundamentos do Livro VI, elencados no art. 2.027-E, merecem transcrição por serem centrais para a compreensão do fenômeno dos *dark patterns*:

> *Art. 2.027-E. São fundamentos da disciplina denominada direito civil digital: I — o respeito à privacidade, à proteção de dados pessoais e patrimoniais, bem como à autodeterminação informativa; II — a liberdade de expressão, de informação, de comunicação e de opinião; III — a inviolabilidade da intimidade, da honra, da vida privada e da imagem da pessoa; IV — o desenvolvimento e a inovação econômicos, científicos e tecnológicos, assegurando a integridade e a privacidade mental, a liberdade cognitiva, o acesso justo, a proteção contra práticas discriminatórias e a transparência algorítmica; [...] VII — o efetivo respeito aos direitos humanos, ao livre desenvolvimento da personalidade e dignidade das pessoas e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2025).*

A leitura do inciso IV é particularmente reveladora: ao consagrar expressamente a liberdade cognitiva e a integridade mental como fundamentos do direito civil digital, o PL 4/2025 eleva à categoria normativa o bem jurídico que os *dark patterns* sistematicamente agridem. Essa escolha reflete a percepção do legislador de que o ambiente digital impõe riscos específicos à formação autônoma da vontade, os quais as categorias tradicionais do direito privado não conseguem capturar.

Não menos importante é o art. 2.027-D, cujo teor merece reprodução:

> *Art. 2.027-D. A tutela dos direitos de personalidade, como salvaguarda da dignidade humana, alcança outros direitos e deveres que surjam do progresso tecnológico, impondo aos intérpretes dos fatos que ocorram no ambiente digital atenção constante para as novas dimensões jurídicas deste avanço. (BRASIL, 2025).*

Essa cláusula de abertura tem função dupla: impede a obsolescência do rol protetivo diante da aceleração tecnológica e impõe ao intérprete a aplicação criativa de categorias existentes para casos imprevistos. O *dark pattern*, técnica em constante evolução, é precisamente o fenômeno alcançado por tal dispositivo. A proteção constitucional desses direitos foi sedimentada pela EC n.º 115/2022, que inseriu a proteção de dados pessoais no art. 5.º da CF. Antes disso, o STF (ADIs 6387 e 6388) já reconhecera a autonomia da autodeterminação informativa em relação à privacidade. O PL 4/2025, ao prever tal fundamento no art. 2.027-E, I, conecta a norma civil diretamente a esse núcleo constitucional.

3.3.2. A Vedação Expressa Ao Design Manipulativo: Análise dos Arts. 2.027-F, 2.027-O e 2.027-T

Se o art. 2.027-E estabelece os fundamentos axiológicos do Livro VI, os arts. 2.027-F, 2.027-O e 2.027-T convertem esses valores em vedações diretas ao design manipulativo. A análise conjunta desses dispositivos revela que o PL 4/2025 cria, de forma inédita no Brasil, uma moldura normativa específica para os *dark patterns*. O art.

2.027-F, § 1.º, III, estabelece como parâmetro fundamental de interpretação de todos os atos no ambiente digital:

> *§ 1.º São parâmetros fundamentais para a interpretação dos fatos, atos, negócios e atividades civis que tiverem lugar no ambiente digital, para apuração de sua licitude e regularidade, os seguintes critérios que atendam aos princípios gerais de direito: [...] III — a garantia da segurança do ambiente digital, revelada pelos sistemas de proteção de dados, capazes de preservar os usuários contra investidas que limitam o discernimento, ainda que momentaneamente. (BRASIL, 2025).*

A precisão da expressão "ainda que momentaneamente" é juridicamente determinante. Os *dark patterns* não eliminam o discernimento do usuário de forma definitiva, mas o suprimem no exato instante da decisão. O *confirmshaming* atua por segundos, tempo suficiente para que a culpa induzida leve ao clique; a pré-seleção opera antes da plena compreensão do formulário; e o *roach motel* aproveita a fadiga cognitiva para inviabilizar a saída. Ao incluir essa ressalva, o legislador demonstra compreender com rigor técnico o mecanismo dessas práticas.

O art. 2.027-O introduz os neurodireitos no ordenamento civil, estabelecendo que são parte indissociável da personalidade e recebem a mesma proteção desta, sendo, portanto, intransmissíveis e irrenunciáveis. O § 2.º elenca os neurodireitos garantidos, incluindo:

> *I — direito à liberdade cognitiva, vedado o uso de neurotecnologias de forma coercitiva ou sem consentimento; [...] III — direito à integridade mental, entendido com o direito à não manipulação da atividade mental por neurotecnologias, vedada a alteração ou eliminação do controle sobre o próprio comportamento sem consentimento. (Brasil, 2025).*

Rigorosamente, os *dark patterns* não operam por neurotecnologias em sentido estrito. Contudo, a inclusão da liberdade cognitiva como neurodireito indissociável da personalidade possui efeito hermenêutico fundamental: estabelece que tal liberdade é um bem jurídico protegido em si mesmo, independentemente do meio tecnológico que a ameace. O art. 2.027-D, ao determinar que a tutela da personalidade alcança novos direitos decorrentes do progresso tecnológico, serve de vetor para essa extensão interpretativa.

É, no entanto, o art. 2.027-T que constitui a vedação mais direta e inequívoca ao design manipulativo:

> *Art. 2.027-T. As interfaces de aplicações digitais deverão possibilitar às pessoas a escolha livre e informada das transações realizadas no ambiente digital, não podendo ser projetadas, organizadas ou operadas de forma a manipular as pessoas, em violação à boa-fé objetiva e à função social. (BRASIL, 2025).*

O dispositivo opera em três camadas normativas simultâneas: impõe uma obrigação positiva às plataformas (possibilitar escolha livre e informada); estabelece uma proibição negativa (não projetar, organizar ou operar de forma manipulativa); e ancora a vedação nos princípios gerais do direito privado (boa-fé objetiva e função social). O verbo "operadas" é especialmente relevante, pois alcança não apenas o design original da interface, mas também seu funcionamento concreto. Em conjunto, os arts. 2.027-F, 2.027-O e 2.027-T criam a moldura normativa que Ramadas (2023, p. 30) e Guerra e Wienskoski (2024, p. 153) identificaram como ausente no ordenamento anterior ao PL.

3.4. Consequências Jurídicas e o Privacy By Design Como Resposta Estrutural

O uso de *dark patterns* produz consequências jurídicas em três planos simultâneos no ordenamento brasileiro. No plano da invalidade, o consentimento obtido por meio de design manipulativo é nulo de pleno direito, por força conjunta do art. 8.º, § 6.º, da LGPD, que determina que o "consentimento obtido com violação às normas desta Lei é nulo" (BRASIL, 2018), e do art. 166, incisos II e IV, do Código Civil, que considera nulo o negócio jurídico cujo objeto ou motivo determinante sejam ilícitos. A nulidade opera retroativamente: todo o tratamento de dados torna-se ilícito, os dados devem ser eliminados, e o titular possui o direito de revogar o consentimento a qualquer tempo, nos termos do art. 18, IX, da LGPD.

No plano da responsabilidade civil, o art. 42 da LGPD impõe ao controlador responsabilidade objetiva pelos danos causados ao titular, dispensando a comprovação de culpa e exigindo apenas a demonstração do dano e do nexo de causalidade com o design

manipulativo adotado. Paralelamente, os arts. 12 e 14 do Código de Defesa do Consumidor estabelecem a responsabilidade objetiva do fornecedor pelo fato do serviço, tratando o *dark pattern* como defeito do serviço digital e vedando, pelo art. 88, a denunciação da lide ao designer responsável pelo desenvolvimento técnico. Soma-se a isso o regime proposto pelos arts. 927-A e 944-A do Código Civil reformado pelo PL 4/2025, que introduz a função pedagógica da responsabilidade civil, permitindo ao magistrado fixar sanção pecuniária de até o quádruplo do dano em hipóteses de reiteração de condutas lesivas.

No plano sancionatório administrativo, a Autoridade Nacional de Proteção de Dados dispõe, com fundamento no art. 52 da LGPD, de um conjunto de medidas que inclui advertências, multas de até 2% do faturamento da pessoa jurídica, limitadas a R$ 50 milhões por infração, publicização da infração, bloqueio do tratamento de dados e determinação de sua eliminação. O guia “Cookies e Proteção de Dados Pessoais”, publicado pela ANPD em outubro de 2022, representa o primeiro sinal regulatório indireto de um órgão público brasileiro acerca de práticas de design enganoso, demonstrando que o tema já integra o campo de preocupação da autoridade fiscalizadora, ainda que inexista, até o momento, arcabouço sancionatório específico voltado ao fenômeno (Guerra; Wienskoski, 2024, p. 149).

A resposta normativa repressiva, embora necessária, revela-se insuficiente quando analisada isoladamente para enfrentar um fenômeno que se transforma em velocidade superior à da produção legislativa. A resposta estrutural encontra-se no Privacy by Design, princípio consagrado no art. 25 do GDPR, sintetizado por Cavoukian (2011, p. 1) como o mandamento que “obriga o controlador a

implementar medidas técnicas e operacionais fim-a-fim completas" para "integrar as salvaguardas no tratamento para proteger os direitos dos titulares", exigindo que a proteção de dados seja incorporada ao design dos sistemas desde sua concepção, e não apenas como correção posterior de falhas já consolidadas.

O PL 4/2025, ao estabelecer no art. 2.027-T que as interfaces devem "possibilitar às pessoas a escolha livre e informada" e ao vedar que sejam "projetadas, organizadas ou operadas de forma a manipular as pessoas, em violação à boa-fé objetiva e à função social", consagra o Privacy by Design no direito civil brasileiro, inserindo o país no movimento global de regulação estrutural já observado no Digital Services Act europeu (2024), no California Privacy Rights Act norte-americano (2023) e nas diretrizes da autoridade indiana de proteção de dados (2023). Todos esses instrumentos convergem para a mesma conclusão: apenas um design ético, concebido desde a origem dos sistemas digitais, é capaz de assegurar um consentimento verdadeiramente livre e genuíno na economia contemporânea de dados (Guerra; Wienskoski, 2024, p. 147).

4. CONCLUSÃO

A análise empreendida neste artigo permitiu demonstrar que o ordenamento jurídico brasileiro já dispunha, antes mesmo do PL 4/2025, de fundamentos normativos suficientes para reconhecer a antijuridicidade dos *dark patterns*. O art. 5.º, XII, da LGPD, ao exigir que o consentimento seja livre, informado e inequívoco, e o art. 39, IV, do CDC, ao vedar o prevalecimento sobre a vulnerabilidade do consumidor, formam conjuntamente uma moldura protetiva que os *dark patterns* violam de maneira sistemática. Os precedentes do CONAR de 2022 e 2023 confirmam que essa conclusão não é

meramente especulativa: a aplicação analógica dos institutos já existentes mostrou-se suficiente para que o órgão identificasse e sancionasse práticas de interface manipulativa como condutas abusivas relacionadas à arquitetura de decisão online.

O problema não residia, portanto, na ausência de normas, mas na inexistência de um comando jurídico suficientemente explícito para produzir uniformidade interpretativa entre os órgãos competentes e assegurar maior segurança jurídica aos controladores de dados. Essa lacuna é precisamente o que o PL 4/2025 busca enfrentar ao inserir, no art. 2.027-T do Código Civil, a vedação de que interfaces digitais sejam "projetadas, organizadas ou operadas de forma a manipular as pessoas, em violação à boa-fé objetiva e à função social", além de estabelecer, no art. 2.027-F, § 1.º, III, que os sistemas de proteção de dados devem preservar os usuários contra investidas capazes de limitar o discernimento "ainda que momentaneamente".

A solução proposta neste artigo para o problema identificado não é essencialmente normativa, pois ela já se encontra em processo de consolidação legislativa pelo próprio PL 4/2025. A solução é, sobretudo, interpretativa: o operador do direito deve tratar os *dark patterns* não como mero problema de design a ser solucionado pelos desenvolvedores de plataformas digitais, mas como questão de licitude do negócio jurídico, a ser analisada caso a caso, com fundamento no tripé normativo formado pelo art. 8.º, § 6.º, da LGPD, pelo art. 39, IV, do CDC e pelo art. 2.027-T do PL 4/2025. Quando o design de uma interface tornar objetivamente mais difícil recusar o consentimento do que concedê-lo, independentemente da intenção do controlador, o consentimento obtido será nulo e o tratamento de dados correspondente tornar-se-á ilícito.

O critério prático para essa aferição pode ser extraído da própria estrutura normativa examinada ao longo da pesquisa: uma interface viola o art. 2.027-T sempre que a assimetria de esforço entre aceitar e recusar o tratamento de dados não puder ser justificada por razão técnica legítima. Plataformas que exigem um clique para aceitar todos os cookies e múltiplas etapas para recusá-los, que apresentam caixas de opt-in previamente marcadas ou que associam a recusa a mensagens constrangedoras não apenas realizam escolhas inadequadas de design. Na realidade, praticam ato ilícito apto a viciar o consentimento, gerar responsabilidade objetiva nos termos do art. 42 da LGPD e ensejar sanções administrativas que podem alcançar R$ 50 milhões por infração perante a ANPD.

A principal limitação deste estudo reside na ausência de precedentes judiciais consolidados sobre o tema no Brasil, circunstância que não enfraquece as conclusões alcançadas, mas evidencia o campo em que a pesquisa jurídica ainda precisará avançar. À medida que a ANPD amadurecer sua atuação sancionatória e que o PL 4/2025 concluir sua tramitação legislativa, será possível verificar se o critério da assimetria de esforço aqui proposto encontrará respaldo consistente na prática decisória das autoridades competentes. Por ora, a conclusão que os dados permitem sustentar é clara: o usuário que clicou em “Aceitar todos” porque não encontrou alternativa acessível e equivalente não consentiu de forma livre, mas foi conduzido por mecanismos de manipulação digital. E o direito brasileiro, interpretado em sua integralidade sistemática, já dispõe de instrumentos suficientes para reconhecer essa violação.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Maria Eduarda Cavalcante Ferreira. **Consentimento no mundo virtual:** como os *dark patterns* influenciam para que ele não seja livre, informado e inequívoco. 2022. Monografia (Graduação em Direito), Faculdade Baiana de Direito, Salvador, 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 maio 2026.

BRASIL. **Lei n.º 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 8 maio 2026.

BRASIL. **Lei n.º 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 8 maio 2026.

BRASIL. **Lei n.º 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 9 maio 2026.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 9 maio 2026.

BRASIL. Senado Federal. **Projeto de Lei n.º 4, de 2025.** Altera a Lei n.º 10.406, de 10 de janeiro de 2002 (Código Civil), para introduzir o Livro do Direito Civil Digital e tratar de negócios e responsabilidade civis nos ambientes digitais. Brasília, DF: Senado Federal, 2025. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/163663. Acesso em: 10 maio 2026.

BRASIL. Supremo Tribunal Federal (STF). **Medida cautelar nas Ações Diretas de Inconstitucionalidade n.º 6387 e 6388.** Relatora: Min. Rosa Weber. Brasília, DF: STF, 2020.

BRIGNULL, Harry. **Deceptive patterns: exposing the tricks tech companies use to control you.** London: Testimonium Ltd, 2023. ISBN 978-1-739454-40-1.

CAVOUKIAN, Ann. ***Privacy by design:*** *the 7 foundational principles*. Rev. ed. Toronto: Information and Privacy Commissioner of Ontario, jan. 2011. Disponível em: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf. Acesso em: 11 maio 2026.

LUPIÁÑEZ-VILLANUEVA, Francisco et al. ***Behavioural study on unfair commercial practices in the digital environment***: dark patterns and manipulative personalisation: final report. Luxemburgo:

Publications Office of the European Union, 2022. Disponível em: https://data.europa.eu/doi/10.2838/859030. Acesso em: 11 maio 2026.

SAMPAIO, Marília de Ávila e Silva; JANDREY, Cláudio Luiz. ***Dark patterns* e seu uso no mercado de consumo.** Revista de Direito do Consumidor, São Paulo, v. 143, p. 231-257, set./out. 2022.

BRIGNULL, Harry. ***Deceptive patterns:*** *exposing the tricks tech companies use to control you.* [S.l.]: Brignull, 2023.

CALIFORNIA. ***California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA).*** Cal. Civ. Code § 1798.100 et seq. Sacramento: State of California, 2020. Disponível em: https://leginfo.legislature.ca.gov. Acesso em: 10 maio 2026.

CONAR**, Conselho Nacional de Autorregulamentação Publicitária. Representação n.º 203/22** (Drogaria São Paulo — Semana Infantil com 80% off na 2.ª unidade). Relatora: Conselheira Camila Felix. Sétima Câmara. Decisão: alteração e advertência. Julgamento: dez. 2022.

CONAR, **Conselho Nacional de Autorregulamentação Publicitária. Representação n.º 233/22** (Monetizze Impulsionadora de Vendas On Line e Umbrella Business). Relator: Conselheiro Vitor Morais de Andrade. Sétima Câmara. Decisão: sustação e advertência. Julgamento: mar. 2023.

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

GONZAGA, Heitor Ferreira. **A juridicidade e a regulamentação dos *dark patterns***. 2022. Trabalho de Conclusão de Curso (Graduação em Direito), Faculdade CESUSC, Florianópolis, 2022.

GUERRA, Sérgio; WIENSKOSKI, Leticia. ***Dark patterns***: uma nova agenda regulatória para o Brasil? A&C, Revista de Direito Administrativo & Constitucional, Belo Horizonte, ano 24, n. 98, p. 137-160, out./dez. 2024.

KAHNEMAN, Daniel. **Rápido e devagar:** duas formas de pensar. Rio de Janeiro: Objetiva, 2012.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Metodologia do trabalho científico.** 9. ed. São Paulo: Atlas, 2021.

MARQUES, Claudia Lima. **Contratos no Código de Defesa do Consumidor:** o novo regime das relações contratuais. 6. ed. São Paulo: Revista dos Tribunais, 2011.

MARQUES, Cláudia Lima; MIRAGEM, Bruno. **O novo direito privado e a proteção dos vulneráveis.** São Paulo: Revista dos Tribunais, 2012.

MATHUR, Arunesh; MAYER, Jonathan; KSHIRSAGAR, Mihir. What makes a dark pattern... dark? Design attributes, normative considerations, and measurement methods. *In*: **CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS,** 2021, Yokohama. Proceedings... New York: ACM, 2021. p. 1-18. DOI: https://doi.org/10.1145/3411764.3445610.

NOUWENS, Midas; LICCARDI, Ilaria; VEALE, Michael; KARGER, David; KAGAL, Lalana. *Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence. In:* ***Proceedings of the 2020***

CHI Conference on Human Factors in Computing Systems, Honolulu, 2020. Anais... Honolulu: ACM, 2020. p. 1-13. Disponível em: https://doi.org/10.1145/3313831.3376321. Acesso em: 11 maio 2026.

OCDE, Organização para a Cooperação e o Desenvolvimento Econômico. ***Dark commercial patterns.*** OECD Digital Economy Papers, Paris, n. 336, 2022.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO. **Dark commercial patterns.** Paris: OCDE, 2022. (OECD Digital Economy Papers, n. 336). Disponível em: https://doi.org/10.1787/44f5e846-en. Acesso em: 15 maio 2025.

RAMADAS, Lucas Sérvio Gonçalves. **Os padrões obscuros "*dark patterns*" no e-commerce brasileiro.** Dissertação (Mestrado Profissional em Direito Econômico e Desenvolvimento), Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), Brasília, 2023.

THALER, Richard H.; SUNSTEIN, Cass R. ***Nudge:*** *improving decisions about health, wealth, and happiness.* New Haven: Yale University Press, 2008.

THALER, Richard H.; SUNSTEIN, Cass R.; BALZ, John P. *Choice architecture. In: SHAFIR, Eldar (org.).* ***The Behavioral Foundations of Public Policy.*** *Princeton*: Princeton University Press, 2013. p. 428-439.

TREVISOL, Gabriel. ***Dark patterns*** **e a proteção do consumidor:** padrões obscuros em plataformas de comércio eletrônico. 2023. Trabalho de Conclusão de Curso (Graduação em Direito), Universidade Federal de Santa Catarina, Florianópolis, 2023.

TVERSKY, Amos; KAHNEMAN, Daniel**. Judgment under uncertainty: heuristics and biases. Science,** Washington, DC, v. 185, n. 4157, p. 1124-1131, set. 1974. Disponível em: http://www.jstor.org/stable/1738360. Acesso em: 11 maio 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais (GDPR). Jornal Oficial da União Europeia, Bruxelas, 4 maio 2016. Disponível em: https://eur-lex.europa.eu. Acesso em: 12 maio 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022.** Lei dos Serviços Digitais (Digital Services Act). Jornal Oficial da União Europeia, Bruxelas, 27 out. 2022. Disponível em: https://eur-lex.europa.eu. Acesso em: 14 maio 2026.

VALIM, Thalles Ricardo Alciati. **Resenha: da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados,** de Danilo Doneda. Inova Jur, Revista Jurídica da UEMG, Belo Horizonte, v. 1, n. 1, p. D1-D13, jan./jun. 2022.

Artigo apresentado ao Curso de Direito do Centro Universitário Santa Terezinha - CEST, para obtenção do grau de Bacharel em Direito.