UNIVERSIDADE FEDERAL DE JUIZ DE FORA

FACULDADE DE DIREITO

MESTRADO EM DIREITO E INOVAÇÃO

Gustavo Carvalho Machado

Dark patterns **e dados pessoais:** uma análise da utilização de padrões enganosos no design de interfaces à luz do regime de proteção de dados brasileiro.

Juiz de Fora

2023

Gustavo Carvalho Machado

***Dark patterns* e dados pessoais:** uma análise da utilização de padrões enganosos no design de interfaces à luz do regime de proteção de dados brasileiro.

Dissertação apresentada ao Programa de Pós-graduação em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito para a obtenção do título de Mestre em Direito. Área de concentração: Direito e Inovação.

Orientador: Prof. Dr. Sérgio Marcos Carvalho de Ávila Negri

Juiz de Fora

2023

Ficha catalográfica elaborada através do programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Machado, Gustavo Carvalho.
Dark patterns e dados pessoais : uma análise da utilização de padrões enganosos no design de interfaces à luz do regime de proteção de dados brasileiro / Gustavo Carvalho Machado. -- 2023.
92 f. : il.

Orientador: Sérgio Marcos Carvalho de Ávila Negri
Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Direito. Programa de Pós-Graduação em Direito, 2023.

1. Design de interface. 2. Dark pattern. 3. Titular como agente vulnerável. 4. Direito à proteção de dados pessoais. I. Negri, Sérgio Marcos Carvalho de Ávila , orient. II. Título.

Gustavo Carvalho Machado

***Dark patterns* e dados pessoais:** uma análise da utilização de padrões enganosos no design de interfaces à luz do regime de proteção de dados brasileiro

Dissertação apresentada ao Programa de pós-graduação em Direito da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do título de Mestre em Direito. Área de concentração: Direito e Inovação

Aprovada em 14 de novembro de 2023.

BANCA EXAMINADORA

Prof. Dr. Sergio Marcos Carvalho de Ávila Negri - Orientador

Universidade Federal de Juiz de Fora

Prof. Dr. Wagner Silveira Rezende

Universidade Federal de Juiz de Fora

Profa. Dra. Caitlin Sampaio Mulholland

PUC Rio de Janeiro

Juiz de Fora, 10/11/2023.

Documento assinado eletronicamente por **caitlin sampaio mulholland**, **Usuário Externo**, em 17/11/2023, às 14:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Sergio Marcos Carvalho de Avila Negri**, **Professor(a)**, em 04/12/2023, às 14:07, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Wagner Silveira Rezende**, **Professor(a)**, em 02/01/2024, às 14:56, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no Portal do SEI-Ufjf (www2.ufjf.br/SEI) através do ícone Conferência de Documentos, informando o código verificador **1571196** e o código CRC **F6D8BC33**.

DEDICATÓRIA

À minha amada esposa, Camila, minha inspiração e maior incentivadora.

AGRADECIMENTOS

A dissertação de mestrado ora apresentada é fruto de muito esforço e a concretização de um sonho pessoal antigo, mas que eu não teria conseguido sem o auxílio de pessoas muito especiais, às quais venho fazer minhas singelas homenagens.

Primeiramente gostaria de fazer um agradecimento especial à minha amada esposa, Camila, com quem tenho o privilégio de dividir a vida, pelo apoio incondicional e por sempre fazer seus os meus sonhos.

Agradeço a meus pais, Derly e Ednilza, e meus irmãos por sempre me apoiarem e se fazerem presentes, mesmo à distância, em especial ao meu irmão, Diego, que sempre foi uma referência acadêmica para mim, e que gentilmente se dispôs a dialogar diversas vezes sobre o tema, trazendo muitas provocações e reflexões.

Também desejo expressar minha gratidão a meus amigos e sócios – necessariamente nessa ordem –, Cláudio e Daniel, pelo companheirismo, pelas trocas diárias e por segurarem a "barra" no trabalho quando precisei me ausentar.

Sou grato ao meu orientador, prof. Sérgio Negri, pelas lições e confiança ao longo dessa jornada, e aos meus companheiros de mestrado, Nathan e Adriane, com quem pude compartilhar os desafios do mestrado, principalmente da escrita da dissertação.

E por fim, gostaria de deixar registrado meu agradecimento a minha cachorrinha, Donatella, pelos nossos passeios diários, que muitas vezes se tornaram momentos de reflexão sobre minha pesquisa.

RESUMO

A presente dissertação visa analisar a utilização dos denominados *dark patterns* no design de interfaces de usuário no direito brasileiro, especificamente diante do regime de proteção de dados pessoais do país. Trata-se de revisão bibliográfica de caráter exploratório, realizada a partir da análise de textos e documentos de natureza jurídica e de campos diversos, como economia comportamental e *human-computer interaction*. O trabalho possui três capítulos. O primeiro capítulo traça a evolução e desenvolvimentos dos direitos à privacidade e a proteção dos dados pessoais, destacando a centralidade atribuída ao controle exercido pelo indivíduo sobre suas informações nas legislações de proteção de dados globais, e como tal controle parte do pressuposto do titular de dados como agente racional. A partir disso, delineia-se a construção do titular como um sujeito vulnerável e suscetível à manipulação. Essa formulação teórica está em consonância com a visão de que o controle individual é insuficiente para garantir efetivamente a salvaguarda dos dados pessoais. No segundo capítulo, por sua vez, desenvolve-se a influência do design de interfaces nas tomadas de decisões dos usuários/titulares de dados. Nesse contexto, apresentou-se diferentes definições de *dark pattern* e foi verificado que as principais características que o compõe um padrão enganoso são: a) design com caráter manipulativo; b) que afeta diretamente o processo decisório do usuário; c) que seja capaz de causar prejuízo ao indivíduo; d) aplicado com o intuito de beneficiar o fornecedor do produto/serviço. Foi apresentado, ainda, exemplos de vieses cognitivos que podem explorados por esses padrões, bem como apresentada uma taxonomia de *dark patterns,* além de tipos específicos de padrões obscuros utilizados no contexto de tratamento de dados pessoais. Por fim, o terceiro capítulo propõe uma avaliação da aplicação dos *dark patterns* à luz do regime de proteção de dados brasileiro, tendo, portanto, a LGPD como parâmetro. A avaliação foi proposta a partir de três elementos: a) princípio da boa-fé objetiva; b) hipóteses de tratamento de dados, notadamente o consentimento; e c) princípio do *privacy by design*. Concluiu-se que a utilização de *dark patterns* afronta diretamente princípios elementares do direito à proteção dos dados pessoais.

Palavras-chave: Design de interface. *Dark pattern*. Titular como agente vulnerável. Direito à proteção de dados pessoais.

ABSTRACT

The present dissertation aims to analyze the use of dark patterns in user interface design under the Brazilian law, specifically under the national framework of personal data protection. It is an exploratory literature review conducted through the analysis of legal texts and documents from various fields, such as behavioral economics and human-computer interaction. The work has three chapters. The first chapter outlines the development of the rights to privacy and data protection, highlighting the centrality attributed to the control exerted by the individual over their information in global data protection legislations, with such control rooted in the assumption of the data subject as a rational agent. From this standpoint, the construction of the data subject as a vulnerable and susceptible individual to manipulation is delineated. This theoretical formulation aligns with the view that individual control is insufficient to effectively ensure the safeguarding of personal data. In the second chapter, the influence of interface design on the decision-making of users/data subjects is explored. Within this context, various definitions of dark patterns are presented, and it is observed that the main characteristics comprising deceptive patterns are: a) design with manipulative intent; b) direct impact on the user's decision-making process; c) ability to cause harm to the individual; d) applied with the aim of benefiting the product/service provider. Additionally, cognitive biases that can be exploited by these patterns are illustrated, alongside a taxonomy of dark patterns and specific types used within the context of personal data processing. Lastly, the third chapter proposes an evaluation of the application of deceptive patterns under the Brazilian data protection regime, employing the LGPD as a parameter. The assessment is based on three elements: a) principle of good faith; b) data processing legal basis, notably consent; and c) privacy by design principle. It is concluded that the use of dark patterns directly challenges fundamental principles of the right to personal data protection.

Keywords: Human-interface design. Dark pattern. Data subject as a vulnerable individual. Right to personal data protection.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
CCPA	*California Consumer Privacy Act*
CDC	Código de Defesa do Consumidor
CF/88	Constituição Federal de 1988
CMA	*Competition and Markets Authority*
CNIL	*Comission Nationale Informatique & Libertés*
CCPA	*California Consumer Privacy Act*
CPRA	*California Privacy Rights Act*
DSA	*Digital Service Act*
EDPB	*European Data Protection Board*
ENISA	*European Network and Information Security Agency*
FIPPs	*Fair Information Practice Principles*
FTC	*Federal Trade Comission*
GDPR	*General Data Protection Regulation*
GPDP	*Garante per la Protezione dei Dati Persolani*
HCD	*Human-centered design*
HCI	*Human-computer interaction*
HMI	*Human machine interfaces*
LAI	Lei de Acesso à Informação
LCP	Lei do Cadastro Positivo
LGPD	Lei Geral de Proteção de Dados
MCI	Marco Civil da Internet
OECD	*Organization for Economic Co-operation and Development*
PbD	*Privacy by Design*

SUMÁRIO

1 INTRODUÇÃO

Em 2010, o designer Harry Brignull cunhou o termo *dark pattern* (“padrão obscuro”) – atualmente o autor utiliza o termo *deceptive pattern* (padrão enganoso) – para se referir a “uma interface do usuário cuidadosamente elaborada para enganar os usuários a realizarem ações, como comprar seguro junto com sua compra ou se inscrever em cobranças recorrentes." (Brignull, 2023, p.11).

Trata-se de um termo guarda-chuva que se refere a uma ampla variedade de práticas de design, que são empregadas em diversos contextos da web e de formas variadas; podem utilizar diferentes tipos de elementos baseados em design (por exemplo, caixas de diálogo pop-up ou texto embutido; variações de cores e destaque de opções etc.) e elementos baseados em texto (por exemplo, uso de elementos emotivos ou linguagem coercitiva); podem ocorrer em sites de e-commerce, aplicativos, em banners de cookies, ferramentas de pesquisa, jogos online e podem intervir em diferentes etapas de uma transação, como as fases de publicidade, pré-compra, pagamento ou pós-compra. Eles, ainda, podem envolver a coleta e o uso de dados do consumidor e/ou o uso de tecnologias de inteligência artificial, como aprendizado de máquina (OECD, 2022, p.9). Seu objetivo primordial reside em explorar as vulnerabilidades do indivíduo (ex: de percepção, compreensão, emocional, etc) para manipular seu processo de tomada de decisão, prejudicando a sua capacidade de realizar escolhas conscientes.

Com efeito, a interação com qualquer forma de tecnologia está intrinsecamente vinculada ao seu design; design este que possui a capacidade de exercer influência sobre os consumidores de maneiras previsíveis. Muitas vezes, os usuários não se dão conta de que um determinado sistema pode explorar suas vulnerabilidades e levá-los, de forma enganosa, a fazer uma escolha específica (KONSUMENTVERKET, 2021, p.16).

Para Brignull, o surgimento e a evolução dos padrões enganosos podem ser atribuídos a alguns fatores. O primeiro deles é a facilidade de se promover o rastreamento online. Com a internet ficou muito fácil observar e medir o comportamento dos usuários em sites e aplicações. Qualquer um pode se utilizar de ferramentas como Google Analytics, Adobe Analytics e Hotjar para avaliar as interações do usuário, como, por exemplo, quando clica em um anúncio; quando clica em um link; quando um teste gratuito é convertido em uma assinatura; quando uma assinatura é renovada, dentre outras informações. Por conseguinte, tais percepções retornam ao processo de design como modificações destinadas a otimizar as taxas de conversão (Brignull, 2023, p.29), o que sinaliza para o segundo fator, que é a facilidade de se realizar os denominados testes A/B.

O método de teste intitulado A/B consiste essencialmente em uma abordagem que viabiliza a comparação entre diferentes versões de uma interface, produto, texto, entre outros elementos. Tal método possibilita a avaliação para determinar qual das versões alcança um resultado mais favorável. É importante ressaltar que o teste A/B não se encarrega de fazer julgamentos acerca da superioridade ou inferioridade de um design específico em relação ao usuário; sua função é exclusivamente oferecer estatísticas sobre o desempenho de cada alternativa. Deste modo, tem-se que o teste A/B serve como uma porta de entrada para a aplicação dos padrões obscuros, visto que um design de caráter manipulativo tende a obter um desempenho superior em comparação a um design mais imparcial. Em outras palavras, a eficácia da manipulação supera a da persuasão (Brignull, 2023, p.31).

Para fins de exemplificação, considere uma configuração de preferências de usuário relacionada ao recebimento de publicidade. Na primeira versão (A) de uma página web, a interface é projetada de tal forma que o usuário deve marcar uma caixa de seleção para indicar sua concordância com o recebimento de publicidade proveniente de empresas parceiras. Por outro lado, na segunda versão (B) disponibilizada online, a mencionada caixa de seleção já se encontra previamente assinalada por configuração padrão. Tendo em conta que os indivíduos tendem a manter as configurações padrão, e até mesmo a acreditar ser a configuração mais segura, é razoável antecipar que a taxa de "autorizações" será mais alta na versão B.

Como último fator, o autor menciona a replicação dos padrões enganosos. Em termos mais precisos, quando uma entidade observa que outra está obtendo resultados financeiros substanciais, impulsionados pelo emprego de tais padrões enganosos, sem sofrer reprimendas legais ou regulatórias, tende a imitar essa abordagem (Brignull, 2023, p.32).

Indubitavelmente, os padrões enganosos encontram-se profundamente entrelaçados nas dinâmicas comerciais, revelando, inclusive, uma crescente sofisticação. De maneira regular as interações entre fornecedores de produtos ou serviços e os consumidores no ambiente online são intermediadas por tais padrões, que detêm a capacidade de direcionar ou limitar as escolhas e ações desses últimos. Isso inclui aspectos relacionados ao tratamento de suas informações pessoais, muitas vezes levando os usuários a divulgarem dados para além do necessário ou a consentir em desacordo com seus reais interesses.

A disseminação da utilização dos *dark patterns* foi evidenciada em várias pesquisas recentes, nas quais foi observada que sua aplicação tem se dado de forma generalizada em diferentes contextos e plataformas (OECD, 2022, p.17/18):

- Segundo a pesquisa de Mathur et al. (2019), 11,1% de cerca de 11.000 sites populares de comércio eletrônico examinados apresentavam padrões escuros.
- De acordo com a varredura realizada pela Rede Internacional de Execução da Proteção ao Consumidor (ICPEN) em 2019, 24% de 1.754 sites/aplicativos de comércio eletrônico investigados apresentavam "dark nudges" (ICPEN, 2019).
- Conforme varredura realizada em 2021 pela autoridade chilena de proteção ao consumidor (SERNAC), 64% de 103 sites chilenos de comércio eletrônico examinados apresentavam pelo menos um padrão obscuro (SERNAC, 2021).
- Em pesquisa promovida por Radesky et al. (2022]), 80% dos aplicativos infantis populares continham pelo menos um recurso de design manipulativo.
- Segundo o resultado da pesquisa de Di Geronimo et al. (2020), 95% de uma amostra de 240 aplicativos populares continham pelo menos um padrão escuro.
- De acordo com estudo da European Comission (EC) realizado em 2022, 97% dos 75 sites e aplicativos populares de comércio eletrônico na UE continham pelo menos um padrão obscuro (EC, 2022).
- Para Gunawan et al. (2021), todos os 105 serviços online mais populares na Google Play Store que apresentavam um formato de aplicativo e site continham pelo menos um padrão escuro.
- De acordo com Moser, Schoenebeck e Resnick (2019), todos os 200 varejistas on-line mais populares nos EUA continham pelo menos quatro instâncias de "recursos de compra por impulso".

A utilização propagada dos *dark patterns* fez com que tais práticas de design não somente ganhassem espaço em pesquisas de áreas diversas, como Direito, Economia comportamental e *Human-computer interaction* (HCI), como também chamou a atenção principalmente de autoridades de proteção de dados pessoais e de proteção aos consumidores, notadamente na Europa e nos EUA.

Para mencionar casos recentes, no início de 2022, *Facebook* e *Google* foram multados pela *Comission Nationale Informatique & Libertés* (CNIL), autoridade de proteção de dados francesa, por disponibilizarem nos sites *facebook.com*, *google.fr* e *youtube.com* um botão que permitia ao usuário aceitar os *cookies* utilizados nas respectivas páginas, sem, contudo, fornecer uma solução equivalente para recusar os *cookies*. Recusar os cookies exigia múltiplos cliques, enquanto a aceitação demandava apenas um clique[1].

Em outro caso, o *Federal Trade Commission* (FTC) interpôs uma queixa contra a Epic Games, entidade responsável pelo popular jogo *Fortnite*, alegando, entre outras questões, que a empresa empregou práticas consideradas enganosas. A Epic Games implementou medidas

[1] Disponível em: https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance. Acesso em: 30 mai. 2023.

que dificultaram a tarefa de cancelar ou requerer reembolsos por cobranças não autorizadas. Diversos usuários apresentaram queixas, argumentando que a Epic utiliza estratégias de design para desencorajar cancelamentos e reembolsos, ocultando a opção ou tornando-a de difícil identificação. Além disso, de forma intencional, a Epic estabeleceu um processo complexo e prolixo para solicitar reembolsos, ocultando o link relevante na seção "Configurações" e impondo aos usuários etapas desnecessárias, como a obrigação de fornecer justificativa e confirmar a intenção de solicitar um reembolso (Brignull *et al*., 2023, recurso online).

Nesse contexto, emergiram também as primeiras regulamentações que explicitamente abordam os padrões obscuros. Exemplos notáveis são a *California Privacy Rights Act* nos Estados Unidos e a *Digital Service Act* na União Europeia.

No que diz respeito ao cenário brasileiro, não há, até o momento, qualquer disposição ou proibição explícita no sistema jurídico nacional relacionada ao uso de padrões de design obscuros. Além disso, a análise e debate sobre as características e os efeitos dos *dark patterns* ainda são incipientes.

Em estudo publicado recentemente, Laura Schertel Mendes, Cláudia Lima Marques e Laís Bergstein (2023, p.4) sinalizaram que uso de dados pessoais é um ponto de preocupação relacionado aos *dark patterns,* e que esses padrões podem ser considerados ilegais sob a legislação consumerista brasileira, tomando como elemento chave para essa compreensão o reconhecimento do consumidor como vulnerável. Além disso, as autoras indicam que os *dark patterns* também podem ser enquadrados como infrações de ordem econômica, nos termos da Lei nº 12.529/2011, pois a utilização de artifícios enganosos aos consumidores acarretaria dificuldades ao funcionamento ou desenvolvimento dos demais fornecedores de bens e serviços, sendo, assim, prejudiciais à livre concorrência (Marques; Mendes; Bergstein, 2023, p.6).

No que tange aos dados pessoais, convém ressaltar que a aplicação desses padrões de manipulação frequentemente está associada ao processamento de informações pessoais, inclusive havendo *dark patterns* criados especificamente para promover a divulgação excessiva de dados e/ou dificultar sua proteção. Diante disso, é pertinente que a análise da utilização desses artifícios contemple a sua conformidade com a legislação nacional de proteção de dados.

Desta sorte, propõe-se a responder nesse trabalho o seguinte questionamento: *à luz do regime de proteção de dados brasileiro, é legítima a utilização dos considerados dark patterns no design da interface de sites e aplicativos*?

Quanto à abordagem metodológica adotada, optou-se por realizar uma pesquisa teórica com base na perspectiva jurídico-dogmática, guiada pelos métodos (i) histórico-jurídico, (ii) jurídico-comparativo e (iii) jurídico-compreensivo, como delineado por Gustin e Dias (2010, p.20/29). O exame dos *dark patterns* no contexto jurídico do Brasil e a formulação de uma proposta interpretativa e de conexão entre esses padrões de design e o direito à proteção de dados pessoais foram conduzidos por meio de revisão bibliográfica e análise de documentos, abrangendo textos de natureza jurídica, tanto nacionais como internacionais, bem como contribuições de campos diversos, como economia comportamental e *human-computer interaction* (HCI). Importante mencionar que a literatura estrangeira, notadamente de autores da América do Norte e Europa, desempenhou um papel significativo na pesquisa, uma vez que o debate sobre a utilização de *dark patterns* encontra-se mais consolidado nessas regiões, inclusive resultando em previsões legislativas.

A dissertação foi estruturada em 03 (três) capítulos. No primeiro capítulo (seção 2), é esboçada a importância central atribuída ao controle exercido pelo indivíduo sobre suas informações nas legislações de proteção de dados globais, incluindo a Lei Geral de Proteção de Dados do Brasil (LGPD), e como tal controle pressupõe que o titular dos dados atue de forma racional. No entanto, é verificado que, devido às inerentes limitações do titular, à disparidade informativa entre o titular e as organizações, e à intrincada natureza dos processos de tratamento de dados no cenário digital, o titular é, na realidade, um sujeito vulnerável e suscetível à manipulação, o que resulta, frequentemente, em decisões que podem não estar alinhadas com seus próprios interesses. Essa formulação teórica está em consonância com a visão de que o controle individual é insuficiente para garantir efetivamente a salvaguarda dos dados pessoais.

O segundo capítulo (seção 3), por sua vez, explicita a influência do design de interfaces nas tomadas de decisões dos usuários/titulares de dados; é demonstrado como a arquitetura de escolha construída pode restringir ou influenciar as ações dos titulares. A partir disso, este capítulo se ocupa de apresentar o que é *dark pattern* e como tem sido definido pela academia, por legislações e por autoridades, especialmente as de proteção de dados e de proteção ao consumidor; delinear as principais características que compõem um padrão obscuro; apresentar exemplos de vieses cognitivos que podem explorados por esses padrões, bem como indicar alguns tipos de dark patterns recorrentemente utilizados, com atenção voltada para aqueles que servem como canais de tratamento de dados pessoais.

No último capítulo (seção 4), uma avaliação da empregabilidade dos padrões obscuros no contexto do regime de proteção de dados brasileiro é conduzida. Para essa análise, as

disposições estabelecidas na LGPD foram utilizadas como base de referência. Essa avaliação foi estruturada em três abordagens centrais: a aplicação do princípio da boa-fé objetiva, conforme delineado no *caput* do artigo 6º; as hipóteses nas quais o tratamento de dados é permitido, com especial atenção ao consentimento, considerando que está diretamente relacionado à capacidade de tomada de decisão pelo titular; e o princípio do *privacy by design*. Adicionalmente, é destacado, de maneira breve, o papel da Autoridade Nacional de Proteção de Dados na abordagem dos padrões obscuros.

2 DA PRIVACIDADE À PROTEÇÃO DE DADOS E O PROTAGONISMO DO CONTROLE DO INDIVÍDUO SOBRE O FLUXO DAS INFORMAÇÕES

A participação do indivíduo no gerenciamento do fluxo de suas informações pessoais remonta ao desenvolvimento da doutrina moderna do direito à privacidade e ao surgimento e evolução do direito à proteção de dados pessoais. Embora já tenha tido um maior protagonismo, o controle individual nunca saiu de cena e ainda hoje goza de status de enorme relevância nas leis de proteção de dados pessoais existentes. Em razão disso, e tendo em conta que a compreensão desse poder de ingerência do indivíduo sobre seus dados é essencial para traçarmos os contornos necessários à análise da utilização das denominadas *dark patterns* no design de interfaces de sites e aplicativos, é oportuno, antes de tudo, rememorar como foi a construção e desenvolvimento desses direitos.

2.1. O DESENVOLVIMENTO DOS DIREITOS À PRIVACIDADE E À PROTEÇÃO DE DADOS PESSOAIS E O PAPEL CENTRAL DO INDIVÍDUO

A doutrina moderna do direito à privacidade surgiu com o famoso artigo *The Right to Privacy,* publicado em 1890 pelos advogados Samuel Warren e Louis Brandeis, segundo o qual o direito à privacidade se consubstanciava em um "direito a ser deixado só" (*right to be let alone*) (Warren; Brandeis, 1890, p.193). Preocupados com as câmeras portáteis da Kodak cuja utilização se alastrava e com o jornalismo sensacionalista da época (Solove, 2008, p.15), o direito desenhado pelos autores caracterizava-se como um direito negativo, que visava a proteção da esfera individual contra interferências alheias. Possuía, portanto, caráter fortemente individualista (Mendes, 2014, local. 502) – e até mesmo egoísta (Doneda, 2019, p.30) –, e se assumiu como uma prerrogativa reservada somente a pessoas com elevada projeção social (Doneda, 2019, p.33).

A partir das décadas de 1960 e 1970, essa compreensão de privacidade atrelada ao isolamento ou a tranquilidade se mostrou insuficiente em um contexto caracterizado pelo aumento massivo do fluxo de informações, condicionado pelo avanço tecnológico dos meios de processamento de dados e pela transição do Estado Liberal para o *Welfare State*, que alterou o relacionamento entre Estado e cidadãos (Doneda, 2019, p.33).

Com o Estado de bem-estar social e o avanço da tecnologia, as informações pessoais ganharam maior importância, na medida em que o Estado, mirando a eficiência de políticas públicas e maior controle social, passou a processar uma enorme quantidade de dados pessoais para conhecer a fundo sua população[2], culminando na criação de banco de dados unificados.

Desse modo, o Estado foi quem primeiro passou a utilizar informações pessoais em larga escala, mas o desenvolvimento dos meios de coleta e processamento de dados, e especialmente o barateamento do custo de hardwares e softwares, somado ao esforço de desenvolvedores e fornecedores de expandir o acesso a seus produtos a uma maior gama de usuários, contribuiu para democratizar o acesso a tecnologias de banco de dados sofisticadas e, assim, alargar sua utilização pelo setor privado (Nissembaum, 2009, p.38).

Nesse contexto, a temática de privacidade passou a se estruturar em torno das informações, notadamente, dos dados pessoais (Doneda, 2019, p.172). O direito à privacidade deixou de se estruturar em torno do eixo "pessoa-informação-segredo", passando a se organizar em torno do eixo "pessoa-informação-circulação-controle" (Rodotà, 1995, p.102 *apud* Doneda, 2019, p.41).

Na medida em que o avanço da tecnologia permitia, dentre outras coisas, a manutenção de arquivos computadorizados sobre as pessoas, sinalizando, assim, uma perda por parte dos indivíduos da capacidade de outrora de controlar os fluxos de seus dados, o direito à privacidade passou a ser compreendido como a capacidade do indivíduo de controlar a circulação de informações vinculadas a ele.

---

[2] "Em primeiro lugar, foi o Estado que por primeiro se encontrou na posição de utilizar largamente informações pessoais. Os motivos são razoavelmente claros: um pressuposto para uma administração pública eficiente e o conhecimento tão acurado quanto possível da população (nao por acaso, a formação do *welfare state* seguiu-se um período de voraz demanda por informação pessoal por parte do Estado), o que implica, por exemplo, a realização de censos e pesquisas e o estabelecimento de regras para tornar compulsória a comunicação de determinadas informações pessoais a administração pública. Em relação ao controle, basta acenar as várias formas de controle social que podem ser desempenhadas pelo Estado e que seriam potencializadas com a maior disponibilidade de informações sobre os cidadãos, aumentando seu poder sobre os indivíduos – não e por outro motivo que um forte controle da informação e característica comum aos regimes totalitários" (Doneda, 2019, p.34).

Dentre os estudos e relatórios feitos na época, destaca-se o relevante relatório *Records, Computers and the Rights of Citizens* (1973), elaborado pelo *Advisory Committee on Automated Personal Data Systems*, instituído pelo *Department of Health, Education and Welfare* dos EUA, documento do qual se extraiu o *Code of Fair Information Practices*, que, fundamentado em cinco princípios basilares (transparência, acesso, finalidade, qualidade dos dados e segurança), deu origem aos conhecidos *Fair Information Practice Principles* (FIPPs), que, por sua vez, serviram de inspiração para diversas legislações e instrumentos regulatórios nos anos e décadas seguintes (Machado, 2022, p.33/34); as *FIPP's* são o alicerce das leis modernas de privacidade (Schwartz 1999, p.35).

Tendo como base de sustentação o estabelecimento de ferramentas que possibilitam o direito de participação do indivíduo na decisão sobre o conteúdo dos dados pessoais objeto de tratamento por bancos de dados (Machado, 2022, p.35), o *Code of Fair Information Practices* foi sintetizado e recebido na Europa como "proteção de dados", enquanto no sistema jurídico dos EUA ficou conhecido como forma de "proteção da privacidade" (Agre, 1997, p.2). Por esse motivo, no que diz respeito a política legislativa e regulatória, o discurso e os debates se consolidaram em torno dos conceitos de "privacidade informacional" (information privacy) e "proteção de dados" (data protection) (Bennett; Raab, 2003, p.36).

Na década de 70 surgiram as primeiras legislações destinadas à tutela dos dados pessoais. Entre as precursoras, menciona-se a Lei do *Land* alemão de Hesse, publicada em 1970; o *Datalag* ou *Data Lagen* 289 na Suécia, a primeira lei nacional de proteção de dados pessoais que se aplicava aos bancos de dados do país, publicada em 1973; e o *Privacy Act* norte-americano em 1974 (Doneda, 2019, p.172). Essa primeira geração de leis de proteção de dados surgiu como reação ao processamento eletrônico de dados nas administrações públicas e nas empresas privadas, bem como às iniciativas de concentração dos bancos de dados em grandes bancos de dados nacionais (Mendes, 2014, local. 516). O núcleo dessas leis era a concessão de autorizações por órgãos públicos para a criação e posterior controle desses bancos de dados (Doneda, 2019, p.176). Priorizando o controle rígido dos procedimentos, as normas desse período deixavam para segundo plano a garantia do direito individual à privacidade (Mendes, 2014, local. 673).

Diante da já mencionada democratização dos bancos de dados informatizados e da cada vez mais ampla utilização das tecnologias de processamento de dados pelo setor privado, as leis de primeira geração logo se tornaram ultrapassadas, uma vez que se tornou inviável a proposta de controle baseada em um regime de autorizações (Doneda, 2019, p.176).

Na segunda metade da década de 70 surge, portanto, a segunda geração de leis de proteção de dados, tendo como principal diferencial em relação às leis de primeira geração a estrutura, que não mais se constrói em torno do fenômeno computacional em si, mas se baseia na consideração da privacidade e na proteção de dados pessoais como uma liberdade negativa, a ser exercitada pelo próprio cidadão (Doneda, 2019, p.177). Nas leis de primeira geração, os indivíduos não podiam decidir se seus dados eram processados; eles poderiam meramente retificar informações enganosas ou imprecisas sobre si mesmos. Já nas leis segunda geração, os indivíduos passaram a ter "voz" no processo de tratamento de seus dados por meio de seu consentimento. Delegou-se ao indivíduo explícito poder de decisão para escolher quais de seus dados pessoais seriam usados para quais propósitos (Mayer-Schönberger , 1997, p.227). Outra mudança significativa dá-se no âmbito institucional, com a ampliação dos poderes das autoridades administrativas encarregadas da proteção de dados (Mendes, 2014, local. 589).

Essa evolução legislativa retratou a insatisfação de cidadãos que sofriam com a utilização por terceiros de seus dados pessoais e necessitavam de instrumentos para defender seus interesses de forma direta. Diante disso, criou-se um sistema que fornece instrumentos para o cidadão identificar o uso indevido de suas informações pessoais e propor sua tutela (Doneda, 2019, p.177).

Já na década de 80, surgiu uma terceira geração de leis de proteção de dados, em que a tutela dos dados permaneceu centrada no indivíduo, mas garantindo uma maior participação dele. O marco da terceira geração é a decisão do Tribunal Constitucional Alemão, de 1983, que considerou inconstitucional parte da Lei do Censo promulgada no país, e que popularizou o termo "autodeterminação informativa", consubstanciado na capacidade do indivíduo de decidir por si mesmo sobre o compartilhamento e o uso de seus próprios dados pessoais (Mayer-Schönberger, 1997, p.229).

Conforme ressaltado por Danilo Doneda (2019, p.178), a proteção de dados é compreendida pelas leis dessa geração como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e leva em consideração o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios para se buscar o efetivo exercício da autodeterminação informativa. Tem-se, portanto, que a participação do indivíduo é a mola propulsora da estrutura das leis de terceira geração.

Segundo Laura Schertel, a principal diferença em relação à segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o

armazenamento e a transmissão e não apenas como a opção entre “tudo ou nada” (Mendes, 2014, local. 709/710).

Por fim, surgiram as leis de quarta geração, entres as quais se inclui a Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/2018), que se caracterizam pela busca de complementar as deficiências do enfoque individual marcante das leis das outras gerações. Reconhecendo o desequilíbrio existente entre o indivíduo e as entidades que coletam e processam seus dados, as leis de quarta geração apresentam uma consciência da dificuldade de basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção. Outra importante característica é a disseminação do modelo de autoridades independentes para a aplicação da lei (Doneda, 2019, p.179).

Contudo, ainda que as leis de quarta geração objetivem reduzir o protagonismo do controle individual, o consentimento do titular – que é expressão da ingerência individual – ainda é figura central na abordagem regulatória. Exemplo disso seria que o consentimento passou a ser adjetivado – deve ser livre, informado, inequívoco e para uma finalidade determinada –, desenhando um movimento refratário em torno do papel de relevância do consentimento quase como sendo sinônimo de autodeterminação informativa (Bioni, 2019, p.117).

Para Schertel, essa evolução das gerações de normas de proteção de dados pessoais reflete a tentativa de se buscar um modelo que garanta efetivamente a autodeterminação do indivíduo, não obstante as dificuldades encontradas para tanto (Mendes, 2014, local. 746).

2.2 O CONTEXTO DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Embora o conceito de "proteção de dados pessoais" seja relativamente recente no contexto brasileiro, questões pertinentes a essa temática já se encontravam integradas à prática jurídica nacional, frequentemente associadas aos direitos de privacidade, do consumidor e a outras liberdades individuais (Doneda, 2021, p.29). Disposições referentes a essa temática podem ser identificadas em diversas legislações setoriais e na própria Constituição Federal de 1988 (CF/88). Posteriormente, a Lei Geral de Proteção de Dados (LGPD) foi promulgada com a finalidade de sistematizar as problemáticas relativas ao tratamento de dados pessoais em um conjunto normativo unificado, estabelecendo, assim, um eixo central em torno do qual a disciplina se estrutura (Doneda, 2021, p.37).

2.2.1 Código do Consumidor (CDC)

O Código de Defesa do Consumidor dispõe em seu art. 43 sobre bancos de dados e cadastros de consumidores, estabelecendo o direito do consumidor, como titular dos dados, de acessar suas informações contidas nos cadastros, fichas e registros mantidos pelo fornecedor. Tal acesso é garantido por meio de notificação do consumidor ou por meio de solicitação do mesmo (§2º). Referido artigo também determina que os dados dos consumidores constantes nos cadastros deverão ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, além de estabelecer limites temporais para a retenção de informações negativas (§1º) e garantir ao consumidor o direito de correção de dados inexatos (§3º). O CDC prevê, ainda, o respeito à boa-fé objetiva (art. 4º, III; art. 51, IV), protegendo o consumidor de situações que o coloquem em desequilíbrio exagerado.

Nesse passo, é possível constatar a incorporação no CDC de certos princípios de proteção de dados, como os princípios da *transparência* e da *qualidade dos dados* presentes nos dispositivos supracitados. Outro exemplo seria a presença do princípio da finalidade – que determina que os dados fornecidos pelo consumidor devem ser utilizados exclusivamente para os propósitos que justificaram sua coleta – em virtude da aplicação da cláusula de boa-fé objetiva. (Doneda, 2019. p. 266).

As disposições do CDC demonstram uma preocupação por parte do legislador em buscar um equilíbrio na relação de consumo, estabelecendo restrições ao uso das informações sobre o consumidor por parte dos fornecedores (Doneda, 2019, p.265), e conferindo ao consumidor certa capacidade de exercer controle sobre seus dados, de autodeterminar as suas informações pessoais (Bioni, 2019, p.127).

2.2.2 Lei do Cadastro Positivo (LCP)

A Lei nº 12.414/2011 estabelece as diretrizes para a constituição de uma base de dados contendo informações relacionadas às transações financeiras e histórico de cumprimento de obrigações, com o objetivo específico de embasar a avaliação e a tomada de decisões sobre concessão de crédito.

Inicialmente, a Lei do Cadastro Positivo estabelecia que a inclusão de consumidores em bancos de dados estava condicionada à obtenção prévia do consentimento por parte dos titulares dos dados pessoais. Porém, com a entrada em vigor da Lei Complementar nº 166/2019, aquela foi modificada para permitir a inclusão de consumidores nos bancos de

dados independentemente de sua autorização (art. 4º, I), permitindo, contudo, a possibilidade de o titular solicitar posteriormente a exclusão de seu nome dos referidos bancos de dados (art. 5º, I). A Lei Complementar nº 166/2019 também modificou a Lei 12.414/2011 para possibilitar que o responsável pelo gerenciamento dos dados compartilhe informações cadastrais e de adimplemento com outros bancos de dados (art. 4º, III), sendo o gestor que receber informação equiparável em obrigações e responsabilidades ao agente de tratamento original (art. 9º, §1º).

Além disso, tal qual no CDC, podemos observar no LCP a presença de princípios de proteção de dados, especificamente os princípios da *finalidade*, *qualidade de dados* e *necessidade*. O primeiro pode ser observado no art. 7º, que dispõe que as informações disponibilizadas nos bancos de dados somente poderão ser utilizadas para "realização de análise de risco de crédito do cadastrado" e para "subsidiar a concessão ou extensão de crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco financeiro ao consulente". Em sentido semelhante o art. 5º, VII, determina que as informações não poderão ser utilizadas para qualquer finalidade que não esteja relacionada à concessão de crédito (art. 5º, VII).

A *qualidade dos dados* é identificada no art. 3º, §1º, que determina que os bancos de dados poderão ser compostos apenas por "informações objetivas, claras, verdadeiras e de fácil compreensão". Já o princípio da *necessidade* é verificado no art 3º, §3º, que proíbe as anotações de informações excessivas – aquelas que não estiverem vinculadas à análise de risco de crédito – e sensíveis – aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

Para Bioni (2019, p.129), o quadro normativo proposto pelo LCP restringe a coleta e o uso dos dados pessoais, com o objetivo de capacitar o consumidor a ter controle sobre suas informações pessoais.

2.2.3 Lei de Acesso à Informação (LAI)

A Lei nº 12.527/2011 estabelece as regras e os procedimentos para garantir o acesso dos cidadãos a informações públicas detidas pelo poder público; veio, portanto, para regulamentar o princípio constitucional da transparência.

O texto da lei em questão traz uma definição de informação pessoal bastante similar à presente na LGPD. De acordo com o artigo 4º, inciso IV, informação pessoal é "aquela que diz respeito a uma pessoa física identificada ou identificável". Além disso, o artigo 31 da LAI

estabelece um conjunto específico de regras para a proteção de dados pessoais sob a custódia do poder público, reconhecendo a importância de incluir a proteção de dados mesmo dentro de uma legislação voltada para a regulamentação do princípio da transparência (Doneda, 2021, p.34).

2.2.4 Marco Civil da Internet (MCI)

A Lei nº 12.965/2014 estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Entre os princípios que sustentam a disciplina, destaca-se a proteção à privacidade (art. 3º, II) e a proteção dos dados pessoais (art. 3º, III).

O Marco Civil da Internet posiciona o usuário como o grande protagonista da proteção de seus dados pessoais (Bioni, 2019, p.131), dado que dispõe expressamente que o uso de dados pessoais, bem como seu armazenamento, tratamento e transferência para terceiros dependerá do consentimento livre, expresso e informado do usuário (art. 7º, VII e IX) – o que demonstra, mais uma vez, que a autodeterminação informacional foi o parâmetro normativo escolhido pelo legislador para proteger os dados pessoais (Bioni, 2019, p.132).

Além disso, é assegurado a todo usuário da internet o respeito aos princípios de proteção de dados da transparência e da finalidade, na medida em que estabelece que o responsável pelo tratamento deve fornecer ao usuário informações claras e completas a respeito da coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, indicando ainda que os dados somente poderão ser tratados para finalidades que justifiquem sua coleta e estejam especificadas nos contratos de prestação de serviço ou em termos de uso de aplicações de internet (art. 7º, VIII).

É oportuno destacar que, embora aborde diversos direitos e procedimentos relacionados ao uso de dados pessoais dos usuários da internet, o MCI já sinalizava a necessidade de uma legislação específica sobre proteção de dados, tanto que, ao estabelecer a proteção de dados como princípio, destacou que seria "na forma da lei". Essa referência indicava a intenção do legislador de desenvolver posteriormente uma legislação específica e mais abrangente para regular a proteção de dados pessoais (Doneda, 2021, p.34).

2.2.5 Lei Geral de Proteção de Dados (LGPD)

Através da introdução da Lei Geral de Proteção de Dados (LGPD) no ordenamento jurídico brasileiro, uma série de institutos específicos relacionados à proteção de dados foi

estabelecida. Isso inclui a definição de princípios próprios, direitos dos titulares de dados e uma abordagem inovadora para a proteção desses titulares, através de requisitos de demonstração e prestação de contas. Além disso, são considerados elementos que levam em consideração os riscos envolvidos nas atividades de tratamento de dados, entre outros aspectos relevantes (Doneda, 2021, p.37).

Primeiro ponto de destaque é que a LGPD traz como um de seus fundamentos a autodeterminação informativa (art. 2ª, II), e, seguindo a linha das leis de proteção de dados de quarta geração, prevê um consentimento extensamente adjetivado – consoante art. 6º, o consentimento deve ser uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Porém, diferente do Marco Civil da Internet, que fundamenta os tratamentos de dados pessoais apenas no consentimento do titular, na LGPD, o consentimento é apenas uma das bases legais para o tratamento. O artigo 7º, em particular, estabelece dez bases legais para o tratamento, incluindo o consentimento. Além disso, o artigo 11, que trata do tratamento de dados pessoais sensíveis, prevê sete outras bases que não dependem da autorização do titular.

A LGPD também incorpora em seu âmbito uma série de princípios procedimentais, alguns dos quais já presentes em leis de gerações anteriores, que devem ser rigorosamente observados pelas atividades de tratamento de dados. Conforme estipulado no artigo 6º da referida lei, as atividades de tratamento devem pautar-se pela observância da boa-fé e dos seguintes princípios:

1) *Finalidade:* realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
1) *Adequação:* compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
2) *Necessidade:* limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
3) *Livre acesso:* garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
4) *Qualidade dos dados:* garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

5) *Transparência:* garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
6) *Segurança:* utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
7) *Prevenção:* adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
8) *Não discriminação*: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
9) *Responsabilização e prestação de contas:* demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Para Bioni (2019, p.157), a centralidade do indivíduo está presente na maioria dos princípios em questão, e essa carga principiológica se justifica pela necessidade de empoderar o titular dos dados pessoais com o controle sobre suas informações pessoais e, acima de tudo, com base em sua autonomia de vontade.

Ressalta-se ainda a consagração de uma série de direitos aos titulares de dados (art. 18), tal como o direito de acesso, correção e portabilidade; passando por informação sobre compartilhamento com terceiros, direito de revogação do consentimento ou de oposição – a depender da existência de tratamento de dados fundada em base legal diversa do consentimento –, revisão de decisões tomadas unicamente com base em tratamento automatizado (art. 20), entre outros.

Outro aspecto relevante a ser sublinhado é a inclusão no texto normativo do conceito de *privacy by design*, que, embora não previsto de forma evidente como disposto no Regulamento Geral de Proteção de Dados europeu, é derivado da aplicação do princípio da prevenção (art. 6º, VIII) mencionado acima e pelo previsto no art. 46, §2º, da lei, que estabelece que as medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de proteção de dados pessoais devem ser consideradas desde a fase de concepção do produto ou serviço até a sua execução.

Por fim, seguindo o modelo das demais legislações de proteção de dados da quarta geração, foi constituída a Autoridade Nacional de Proteção de Dados (ANPD), autoridade independente responsável por zelar pela observação da lei.

2.2.6 Constituição Federal (CF/88)

Consoante o disposto no art. 5º, inciso LXXIX, da Constituição Federal de 1988, é assegurado a todos brasileiros e estrangeiros residentes no país o direito à proteção dos dados pessoais. O dispositivo em questão foi acrescentado pela Emenda Constitucional nº 115/2022, alçando o direito à proteção de dados pessoais ao *status* normativo de direito fundamental, reconhecendo-o, portanto, como direito autônomo, cuja tutela vai além da privacidade, estando diretamente vinculado à proteção da personalidade do titular dos dados (Sarlet, 2021, p.41)[3]. Ao equiparar a proteção de dados pessoais aos demais direitos fundamentais, pretendeu-se, portanto, assegurar a salvaguarda da personalidade em sua concepção mais abrangente diante das vicissitudes da Sociedade da Informação (Doneda, 2020, p.270).

Segundo Laura Schertel Mendes (2014, local. 3449), essa proteção pode ser pensada em duas dimensões: uma consiste na proteção do indivíduo contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais, e a outra consiste na atribuição ao indivíduo da garantia de controlar o fluxo de seus dados na sociedade. De outra maneira, a primeira dimensão mencionada é de caráter objetivo e implica no dever do Estado de agir de forma protetiva, estabelecendo condições e procedimentos adequados para assegurar o pleno exercício e desfrute desse direito fundamental, e a segunda é de natureza subjetiva e envolve a liberdade negativa do cidadão, ou seja, a capacidade de se opor à intervenção estatal e preservar seu espaço individual livre de interferências (Mendes *et al,* 2021, p.86).

2.3 TEORIA DO CONTROLE E O TITULAR COMO AGENTE VULNERÁVEL

Com base na síntese histórica apresentada anteriormente, evidencia-se a relevância conferida ao papel do indivíduo no gerenciamento de suas informações, compreendido como

[3] Segundo Laura Schertel Mendes (2014, local. 2238): "A importância da tutela jurídica dos dados pessoais reside no fato de que esses dados, assim como as demais informações extraídas a partir deles, podem se constituir uma representação virtual da pessoa perante a sociedade. (...). Assim, os dados pessoais passam a ser constituintes da própria personalidade do indivíduo, dada a sua importância para a representação das pessoas na sociedade contemporânea.".

autodeterminação informativa, nas legislações de proteção de dados pessoais. Indubitavelmente, entre as diferentes concepções existentes de privacidade[4] e proteção de dados, a teoria do controle sobre as próprias informações emerge como uma das mais amplamente abordadas pela doutrina e exerce significativa influência nas legislações atuais. Em virtude disso, adotaremos a teoria do controle como o referencial para o presente estudo.

Alan Westin, um dos principais expoentes desse entendimento, definiu a privacidade como "a reivindicação de indivíduos, grupos ou instituições de determinar por si próprios quando, como e em que medida as informações sobre eles são comunicadas a outros" (Westin, 1967, p.7). Para o autor, o indivíduo está em um contínuo processo de ajustamento pessoal em que equilibra o desejo de privacidade com o desejo de divulgação e comunicação de si mesmo aos outros, conforme as condições ambientais e das normas sociais estabelecidas pela sociedade em que vive (Westin, 1967, p.7/8).

Em direção semelhante, Arthur Miller sustenta que o atributo básico de um direito efetivo de privacidade é a capacidade do indivíduo de controlar a circulação de informações relacionadas a ele, poder este essencial para manter as relações sociais e a liberdade pessoal (Miller, 1971, p.25).

Charles Fried, por sua vez, escreveu que “privacidade não é simplesmente uma ausência de informação sobre nós na mente dos outros; ao invés disso, é o controle que temos sobre as informações que digam respeito a nós mesmos" (Fried, 1968, p.482 *apud* Borgesius, 2014, p.91, tradução nossa).

Já Paul Schwartz descreve a teoria do controle como um princípio de autonomia liberal cujo objetivo é colocar o indivíduo no centro da tomada de decisões sobre o uso de informações pessoais; que busca alcançar a autodeterminação informacional por meio da administração individual de dados pessoais e mantendo as informações isoladas do acesso (Schwartz, 2000, p.820).

Na visão do professor Michael Birnhack o controle toma a forma do direito dos indivíduos de saber quais informações sobre eles são coletadas; de determinar quais informações podem ser disponibilizadas a terceiros; e de acessar e corrigir seus dados pessoais, se for o caso (Birnhack, 2011 *apud* Lazaro; Métayer, 2015, p.8).

Com efeito, pode-se dizer que há um consenso entre muitos estudiosos e legisladores de que a chave para a privacidade em geral, e proteção de dados especificamente, é o controle

[4] No presente trabalho utilizaremos o termo “privacidade” e “*privacy”* como sinônimos de “privacidade informacional”, cujo conceito e desenvolvimento, como já mencionado, são equivalentes ao de proteção de dados pessoais.

sobre as informações pessoais (Hartzog, 2018a, p.434)[5]. Como ressaltado por Christophe Lazaro e Daniel Le Métayer (2015, p.7), ainda nos dias de hoje o conceito de controle é endossado como a solução chave para os problemas surgidos com as atuais tecnologias de processamento de dados pessoais; é um remédio prescritivo proposto por estudiosos.

Reflexo disso é a importância dada ao controle nas legislações atuais de proteção de dados pessoais. A título de exemplo, o *General Data Protection Regulation (GDPR)* da União Europeia prevê expressamente em seu Considerando nº 7 que pessoas naturais devem ter controle sobre suas próprias informações[6]. Nos Estados Unidos, a *California Privacy Rights Act (CPRA)* prevê que fundamental para o direito de privacidade é a capacidade dos indivíduos de controlar o uso, incluindo a venda, de suas informações pessoais[7]. Destaca-se, também, a Lei Geral de Proteção de Dados brasileira que prevê expressamente em seu art. 2ª que um dos fundamentos da disciplina de proteção de dados é a autodeterminação informativa[8]; além de dispor em seu art. 51 que a "Autoridade Nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais"[9].

A teoria do controle enfatiza, portanto, a liberdade das pessoas de decidir o que deve acontecer com as informações que lhes dizem respeito. Em tese, enxergar a privacidade como controle tem a vantagem de respeitar as preferências individuais das pessoas (Borgesius, 2014, p.90). No entanto, é exatamente por focar tanto no interesse individual que a privacidade sob essa perspectiva de controle também é muito criticada.

Paul Schwartz argumenta que a teoria do controle assume erroneamente que os indivíduos têm autonomia para exercer controle sobre seus dados pessoais em todas as

---

[5] Nas palavras de Schwartz (2000, p.820), "[o] peso do consenso sobre a centralidade do controle de privacidade é impressionante".

[6] "Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.". Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 10 fev. 2023.

[7] SEC. 2. The Legislature finds and declares that: (a) In 1972, California voters amended the California Constitution to include the right of privacy among the "inalienable" rights of all people. The amendment established a legal and enforceable right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information. Disponivel em: https://iapp.org/media/pdf/resource_center/ca_privacy_rights_act_2020_ballot_initiative.pdf. Acesso em: 10 fev. 2023.

[8] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: (...) II - a autodeterminação informativa;

[9] Art. 51. A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais.

situações. O autor questiona a suposição de que os indivíduos são capazes de exercer escolhas significativas em relação às suas informações, dadas as disparidades de conhecimento e poder de barganha sobre a transferências de suas informações (Schwartz, 1999 *apud* Solove, 2008, p.29).

Woodrow Hartzog também defende que o controle do indivíduo é ilusório, isso porque o controle concedido ao indivíduo é mediado, ou seja, ele é projetado para produzir resultados específicos. O autor afirma que, dentro do cenário de tecnologias em escala, os serviços que usamos devem necessariamente ser construídos de uma maneira que restrinja nossas escolhas; e nesse contexto o design tem enorme relevância, uma vez que ele tem a capacidade de afunilar o comportamento do indivíduo, afinal, as pessoas só podem clicar nas opções que lhe são oferecidas (Hartzog, 2018a, p.426).

Nesse cenário, ainda que as empresas se esforcem para tornar o controle do titular de dados significativo, esse comando ainda seria ilusório, isso porque o exercício do controle requer escolha, e essas escolhas são arquitetadas (Hartzog, 2018a, p.427), como será melhor explorado mais adiante.

Referindo-se à ideia de controle como *privacy self-managment*, Daniel Solove assevera que o autogerenciamento não proporciona aos indivíduos um controle significativo. Dentre os motivos apresentados, o autor ressalta que pesquisas empíricas e no campo das ciências sociais demonstram que os indivíduos possuem problemas cognitivos que minam esse pretenso controle; problemas esses que os impedem de fazer escolhas informadas e racionais acerca dos custos e benefícios de consentir com a coleta, uso e divulgação de seus dados pessoais. Outro ponto de preocupação é que mesmo aqueles indivíduos que sejam considerados racionais e bem-informados não conseguem autogerenciar de maneira adequada sua privacidade por conta de vários problemas estruturais, como o fato de o cidadão ter que gerir suas informações perante inúmeras entidades que coletam e tratam seus dados pessoais. Além do mais, é praticamente impossível para as pessoas sopesarem os custos e benefícios de compartilhar seus dados ou permitir sua utilização sem entender o fluxo desses dados e possíveis usos secundários, tornando ainda mais limitada a eficácia da estrutura de autogerenciamento de privacidade (Solove, 2012, p.1880/1881).

Abordando essa visão de privacidade que tem como centro de gravidade o controle das informações a partir de uma compreensão da existência de uma assimetria informacional – e, portanto, uma assimetria de poder – entre organizações e indivíduos, Stefano Rodotà enxerga o controle como um instrumento de equilíbrio na distribuição de poder; mas que esse equilíbrio seria irrealizável se a perspectiva do controle permanecesse somente individual.

Para o autor italiano raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, e que, por conta da enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações que coletam seus dados, é ilusório se falar em controle (Rodotà, 2018, p.37).

Tendo isso em conta, o autor italiano concebe duas dimensões de controle, a individual, caracterizada por esse poder atribuído diretamente ao indivíduo, e a coletiva, que tem como ponto de partida o reconhecimento da limitação de uma proteção fundada unicamente no controle do indivíduo, optando-se, portanto, pela atribuição de um poder geral de vigilância a órgãos criados especificamente para a proteção de dados pessoais (Rodotà, 2018, p.60).

Desponta-se, assim, o papel exercido pelas Autoridades de Proteção de Dados (*Data Protection Authorities – DPA*), recurso presente na maioria dos marcos regulatórios sobre proteção de dados existentes no mundo, cuja atuação fiscalizatória foi prevista na Carta de Direitos Fundamentais da União Europeia de 2000 como parte inerente ao próprio direito fundamental à proteção de dados[10].

As autoridades de proteção de dados sobrevieram principalmente pelo fato de que "os tratamentos de dados e seus efeitos são dificilmente passíveis de serem acompanhados de forma eficaz pelo cidadão ou a necessidade de uma constante atualização em função do desenvolvimento tecnológico" (Doneda, 2019, p.308). Diferentemente das autoridades/agências reguladoras, as autoridades de proteção de dados têm o perfil de autoridade de garantia, cujo propósito é tutelar direitos fundamentais[11], notadamente o direito à proteção de dados pessoais.

---

[10] Artigo 8. Proteção de dados pessoais
1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.
Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. Acesso em: 10 fev. 2023.

[11] Nas palavras de Doneda: "Às autoridades de regulação, cuja competência costuma ser ligada a um determinado serviço de caráter público, são destinadas funções similares àquelas da própria administração pública, com vantagem da dinamicidade de sua estrutura. Por sua vez, as autoridades de garantia (ou simplesmente 'garantes') teriam a missão de ponderar situações subjetivas garantidas pela Constituição e operar um balanceamento dos direitos em questão sem estarem vinculadas ao interesse público administrativo, no sentido de uma valoração 'discricionária'. Um organismo com a proposta de proteção de um direito fundamental estaria enquadrado, portanto, como uma autoridade de garantia." (Doneda, 2019, p.318).

Doneda chama atenção à importância da atuação das autoridades de proteção de dados por considerar que a simples atuação do indivíduo para a proteção de seus interesses (controle individual) não é capaz de fornecer uma tutela adequada. Para o autor é impossível que os direitos que hoje estão relacionados à proteção de dados sejam contemplados unicamente pela ação singular de seu interessado tendo em vista a disparidade entre as possibilidades do indivíduo e as estruturas existentes destinadas ao tratamento de seus dados[12].

Em vista disso, Doneda (2021, p.471) considera que a atuação de uma autoridade de proteção de dados representa instrumento essencial para garantir o respeito e efetivação do direito fundamental à proteção de dados pessoais.

2.3.1 O titular de dados como agente racional *vs* titular de dados como agente vulnerável

Consoante o delineado, a concepção de privacidade como controle individual se fundamenta na liberdade do indivíduo de controlar suas próprias informações; de escolher suas preferências relacionadas à privacidade, como, p.ex., quem poderá ter acesso a seus dados ou com quem irá compartilhá-los. A teoria do controle individual parte do pressuposto, portanto, de que o indivíduo é um agente racional, que consegue sopesar todos os custos e benefícios do compartilhamento de seus dados; que consegue ponderar os impactos que o tratamento de seus dados por diferentes atores terá sobre si.

A propósito, Alan Westin criou um modelo de segmentação de perfis de consumidores[13] com base em suas preocupações com privacidade que exemplifica essa compreensão do titular de dados como sujeito economicamente racional. Para Westin, os consumidores se dividem em "fundamentalistas" (*privacy fundamentalists*), "pragmáticos" (*privacy pragmatics*) e "despreocupados" (*privacy unconcerned*) (Hoofnagle; Urban, 2014a, p.263).

Os fundamentalistas seriam aqueles que enxergam a privacidade como um valor especialmente alto, que rejeitam as alegações de muitas organizações acerca da necessidade

[12] Doneda afirma que a atuação de uma autoridade de proteção de dados é instrumento necessário para a efetivação de uma "garantia institucional", fazendo referência à conceituação de Fábio Konder Comparato, segundo o qual garantias institucionais seriam "formas de organização do Estado, ou institutos da vida social, cuja função é assegurar o respeito aos direitos subjetivos fundamentais, declarados na Constituição; não apenas liberdades fundamentais (...), mas de todas as demais espécies de direitos humanos" (Doneda, 2021, p.471).

[13] Embora o estudo de Alan Westin tenha se concentrado nos consumidores norte-americanos, devido à sua influência na doutrina e nas legislações de proteção de dados, considerou-se pertinente trazer essa segmentação de perfis de consumidores para o presente estudo.

de obter informações pessoais para seus negócios ou programas governamentais, e são favoráveis a promulgação de leis fortes para garantir os direitos de privacidade e controlar a discricionariedade organizacional (Hoofnagle; Urban, 2014a, p.267).

Os despreocupados basicamente seriam aqueles que tem poucos problemas em fornecer suas informações pessoais a autoridades governamentais ou empresas, e não veem necessidade na criação de mais burocracia governamental para proteger a privacidade de alguém (Hoofnagle; Urban, 2014a, p.268).

Já os pragmáticos seriam aquelas pessoas que avaliam o valor, tanto para si como para a sociedade, dos programas empresariais ou governamentais que solicitam informações pessoais, examinam a relevância das informações solicitadas, buscam conhecer os riscos potenciais à privacidade ou à segurança de suas informações, verificam se boas práticas estão sendo observadas e, em seguida, decidem se concordarão ou não com tratamentos específicos de seus dados, sendo que sua confiança no setor ou numa empresa em particular é um fator crítico para essa decisão. Os pragmáticos privilegiam a escolha do consumidor e os padrões adotados pelo mercado em detrimento da legislação e do *enforcement* governamental, mas eventualmente podem apoiar a criação de leis caso entendam necessário (Hoofnagle; Urban, 2014a, p.268).

O trabalho de Westin enquadra a maioria dos consumidores como "pragmáticos", sendo o titular de dados a personificação do *homo economicus* (Hoofnagle; Urban, 2014a, p.264) – um tomador de decisão racional, ponderado, centrado no interesse pessoal e com capacidade ilimitada de processar informações (Avila; Bianchi, 2015, p.14). Adotando uma perspectiva de *leave-it-to-the-market,* o autor aposta no modelo de escolha racional e espera que os próprios consumidores negociem sua privacidade junto ao mercado (Hoofnagle; Urban, 2014, p.264).

Em crítica ao trabalho de Westin, Jennifer Urban e Chris Hoofnagle apontam que a pesquisa em questão era sobre o que o consumidor pensava a respeito de controle, uso de dados pelo mercado e sobre a legislação existente, e não sobre como agiam ao tomar decisões relacionadas à privacidade, de modo que não é possível, por meio do referido estudo, chegar à conclusão de que os pragmáticos colocam na balança os prós e contras do compartilhamento de seus dados, avaliam as proteções aplicadas, dentre outras coisas, para só depois decidir se vão fornecer seus dados (Hoofnagle; Urban, 2014a, p.271).

Os autores sustentam que, na realidade, a maioria dos consumidores tem déficits substanciais em seu conhecimento das leis de privacidade e das práticas comerciais, de modo que normalmente não compreendem a finalidade de uma coleta de dados pessoais e/ou

acreditam que seus direitos estão assegurados simplesmente por estarem previstos em uma política de privacidade, por exemplo. Como consequência, essa miopia causada pelo *gap* de conhecimento pode fazer com que os indivíduos encontrem poucos motivos para negociar sua privacidade no mercado (Urban; Hoofnagle, 2014b, p.1/3).

Urban e Hoofnagle ainda sugerem que a segmentação desenvolvida por Westin deveria ser dividida em dois grupos, os *resilientes* – aqueles com maior conhecimento e maior disposição para proteger sua privacidade – e os *vulneráveis* – aqueles com menor conhecimento e menos propensos a tomar medidas para proteger sua privacidade –, sendo o primeiro grupo composto pelos denominados *privacy fundamentalists* e o segundo formado pelos *privacy pragmatics* e *privacy unconcerned* (Urban; Hoofnagle, 2014b, p.1/3).

Essa abordagem que reconhece o titular como agente racional influenciou sobremaneira o conhecido modelo de "aviso e consentimento" presente em muitas leis de privacidade e proteção de dados e difundido principalmente no ambiente online. Essa combinação de transparência e escolha "parece modelar o controle porque permite que os indivíduos avaliem as opções deliberadamente e então decidam livremente se dão ou não consentimento" (Nissembaum, 2011, p.34).

Em sentido oposto, Harry Brignull aduz que, ao invés de pensar no *homo economicus,* deve-se pensar o indivíduo como *homo manipulable*, ou seja, imperfeito e vulnerável (Brignull, 2023, p. 35).

Nessa direção, Ryan Calo também apresenta o titular de dados como um sujeito vulnerável. De acordo com o autor o conhecimento a respeito do indivíduo confere poder sobre ele, tornando-o vulnerável, servindo a privacidade como uma barreira para evitar a exploração dessa vulnerabilidade (Calo, 2017, p.594/596).

Bruno Bioni (2019, p.162) faz coro a essa compreensão afirmando que em meio ao mercado informacional o cidadão deve ser identificado como um sujeito vulnerável. Para Laura Schertel (2014, local. 3928), essa vulnerabilidade do titular é tanto técnica, por possuir menos informações que o fornecedor de um produto/serviço a respeito do fluxo de seus dados, como fática, na medida em que o indivíduo possui menos recursos intelectuais e econômicos para a reparação de eventuais prejuízos advindos do tratamento de seus dados.

Bruno Miragem ressalta que, para além do déficit de informações, os indivíduos também enfrentam a falta de familiaridade com o ambiente digital. Para o autor, a vulnerabilidade informacional, que está associada à assimetria informacional do consumidor na relação com o fornecedor:

> (...) não se resume à falta ou à pouca qualidade da informação prestada, mas a ausência de habilidade ou familiaridade com o ambiente digital, o que repercute tanto na interpretação das manifestações nele emitidas ou recebidas, quanto na própria capacidade de resposta adequada a seus interesses nas relações jurídicas que resultem daí (Miragem, 2020, p.239)

Neste ponto, é relevante pontuar que para além dessa abordagem universal de vulnerabilidade, amplamente adotada na doutrina consumerista e frequentemente incorporada à doutrina de proteção de dados, existe uma diversidade de titulares de dados que ocupam distintas posições de vulnerabilidade. Eles apresentam variações em termos de compreensão, níveis de consciência, capacidade de decisão, propensão para a divulgação de seus dados e graus de fragilidade. (Malgieri; Niklas, 2020, p.5).

Segundo Gianclaudio Malgieri a vulnerabilidade do indivíduo pode decorrer tanto do próprio tratamento de dados em si, como também dos efeitos causados pelo tratamento de dados (Malgieri; Niklas, 2020, p.5).

Sob a primeira perspectiva, a vulnerabilidade do titular pode advir, por exemplo, de sua capacidade limitada de tomada de decisão, de compreender as informações necessárias a respeito do tratamento de dados ou de exercer seus direitos de forma adequada. Segundo o autor, essa limitação pode resultar de vários fatores, como idade, deficiência ou posição socioeconômica. Já sob a segunda perspectiva, a vulnerabilidade do titular emerge da forma como ele está exposto a danos decorrentes do tratamento de dados. Nesse caso, destaca-se principalmente os titulares integrantes de grupos minoritários, na medida em que tecnologias orientadas a dados tendem a reforçar desigualdades sociais e promover a discriminação no acesso a bens e serviços (Malgieri; Niklas, 2020, p.5).

Também trazendo luz às diferentes camadas de vulnerabilidade a que as pessoas estão submetidas, Joana Machado, Sérgio Negri e Carolina Giovanini (2020) exploram a dimensão política de vulnerabilidade, analisando de forma crítica os impactos – muitas vezes não considerados e/ou não calculados – que o processamento de dados pode acarretar a grupos com vulnerabilidade politicamente induzida.

Nesta pesquisa optar-se-á pelo conceito de vulnerabilidade em seu caráter universal, de modo que as diferentes camadas de vulnerabilidade não serão exploradas. O foco recairá, portanto, principalmente na perspectiva de vulnerabilidade resultante do tratamento de dados em si, que está muito atrelada à assimetria informacional entre indivíduo e organizações. Esse desequilíbrio tem sido objeto de análises em diversos estudos de economia comportamental aplicados à tomada de decisões que envolvem dados pessoais.

De acordo com esses estudos, há uma dicotomia visível entre a percepção dos indivíduos sobre privacidade e a forma como efetivamente se comportam ao tomar decisões relacionadas ao assunto. Exemplo disso é que, quando são questionadas em pesquisas acerca da importância dada à privacidade e à proteção de suas informações pessoais, as pessoas costumam declarar sua preocupação com a temática, mas, em contrapartida, muitas vezes as pessoas sequer leem as políticas de privacidade disponibilizadas nos *sites* e aplicativos que acessam[14], ou mesmo deixam de optar pelo não compartilhamento ou divulgação de seus dados quando têm a opção de fazê-lo; e costumam fornecer seus dados em troca de benefícios muito pequenos (Solove, 2012, p. 1884/1886).

Para Alessandro Acquisti e Jens Grossklags (2005), além de os indivíduos estarem dispostos a trocar privacidade por conveniência ou barganhar a divulgação de informações pessoais em troca de recompensas relativamente pequenas, eles raramente estão dispostos a utilizar tecnologias que visam proteger a privacidade.

Solove (2012, p.1886) afirma que há uma clara desconexão entre o alto valor atribuído à privacidade pelas pessoas quando questionadas a respeito e o seu comportamento, que indica exatamente o contrário.

Segundo Acquisti e Grossklags, a privacidade envolve um problema de decisão complexo que faz com que opiniões, atitudes e comportamentos se difiram substancialmente de um indivíduo para outro. Para os autores, percepções subjetivas de ameaças e danos potenciais, necessidades psicológicas e retornos econômicos desempenham um papel importante nas decisões dos indivíduos de proteger ou compartilhar informações pessoais, motivo pelo qual, por vezes, o comportamento do indivíduo apresenta inconsistências ou mesmo contradições (Acquisti; Grossklags, 2008, p.363).

Fato é que o processo de decisão individual em relação à privacidade é afetado e influenciado por múltiplos fatores, tais como informações incompletas, racionalidade limitada e desvios psicológicos sistemáticos da racionalidade, de maneira que essa pretensa racionalidade pode não capturar as nuances e sensibilidade do comportamento de um indivíduo em relação à sua privacidade (Acquisti; Grossklags, 2005).

Descrevendo os desafios da tomada de decisão, Acquisti e Grossklags apontam que:

---

[14] Segundo pesquisa publicada pelo CETIC.br em 2021, entre os usuários de internet no Brasil dentro da faixa etária de 16 a 24 anos, 27% relataram ler integralmente as políticas de privacidade, 31% leem parcialmente e 35% não leem. Disponível em: https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf. Acesso em: 26 mai. 2023.

> [...] informações incompletas afetam a tomada de decisões de privacidade devido a externalidades (quando terceiros compartilham informações pessoais sobre um indivíduo, eles podem afetar esse indivíduo sem que ele faça parte da transação entre essas partes), assimetrias de informação (informações relevantes para o processo de decisão de privacidade — por exemplo, as informações pessoais que serão usadas podem ser conhecidas apenas por um subconjunto das partes que tomam decisões), risco (a maioria das recompensas relacionadas à privacidade não são determinísticas) e incertezas (as recompensas podem não ser apenas aleatórias, mas dependentes de fatores aleatórios desconhecidos). Os benefícios e custos associados a invasões e proteção de privacidade são complexos, multifacetados e específicos ao contexto. Eles são frequentemente empacotados com outros produtos e serviços (por exemplo, uma consulta de mecanismo de pesquisa pode solicitar o resultado desejado, mas também pode fornecer aos observadores informações sobre os interesses do pesquisador) e geralmente são reconhecidos somente após a ocorrência de violações de privacidade. Eles podem ser monetários, mas também imateriais e, portanto, difíceis de quantificar (Acquisti; Grossklags, 2005, tradução nossa).

Acquisti, Laura Brandimarte e George Loewenstein (2022, p.63) estruturam a vulnerabilidade dos indivíduos diante da tomada de decisões de privacidade em três temas principais: incerteza; dependência do contexto; e maleabilidade e influência.

A principal fonte de incerteza é que as tomadas de decisão relacionadas à privacidade são afetadas por informações incompletas e, em particular, informações assimétricas, isso porque os titulares dos dados geralmente sabem muito menos sobre a magnitude da coleta e uso de dados pessoais compartilhados ou coletados (in)voluntariamente ou (in)conscientemente do que os responsáveis pelo tratamento desses dados (Acquisti; Grossklags, 2008, p. 364), ficando em uma situação desvantajosa.

Soma-se isso ao fato que o complexo ciclo de vida dos dados pessoais na sociedade de informação moderna pode resultar em uma infinidade de consequências que os indivíduos dificilmente são capazes de considerar em sua totalidade (Acquisti; Grossklags, 2008, p. 364). A propósito, Hal Varian aponta que um indivíduo tem pouco ou nenhum controle sobre o uso secundário de suas informações pessoais e, portanto, pode estar sujeito a externalidades sempre que outras partes transacionarem seus dados pessoais (Varian, 1996 *apud* Acquisti; Grossklags, 2008, p.365).

Além da questão da incerteza, as preferências de privacidade são dependentes do contexto. Acquisti, Brandimarte e Loewenstein (2022, p.67) defendem que quando as pessoas não têm certeza sobre suas preferências, elas geralmente procuram pistas que as oriente. E como as pistas são uma função do contexto, o comportamento também é. A depender da

situação, portanto, os indivíduos podem ir da extrema preocupação com sua privacidade à completa apatia. Exemplo disso seria o comportamento diferente de um indivíduo em uma videoconferência com amigos e em uma *live* que ficará gravada e disponível ao público.

No que diz respeito à maleabilidade, os autores observam que vários fatores, às vezes sutis, podem ser usados para ativar ou suprimir preocupações com privacidade, influenciando o comportamento dos indivíduos. Um ótimo exemplo são as configurações-padrão de um site ou aplicativo, que podem influenciar diretamente na divulgação de dados pessoais pelo titular-usuário (Acquisti; Brandimarte; Loewenstein 2022, p.70).

Não restam dúvidas, portanto, que o desequilíbrio informacional é a regra no campo da privacidade (Acquisti *et al,* 2017, p.4); contudo, de acordo com Acquisti e Grossklags (2005, p.2), mesmo que os indivíduos tenham acesso a informações completas, eles não são capazes de tomar decisões apuradas, ainda mais diante de grandes quantidades de dados. Tendo em conta a complexidade e ramificações das consequências associadas à proteção ou divulgação de informações pessoais, a racionalidade limitada (*bounded rationality*) do indivíduo reduz sua capacidade de adquirir, memorizar e processar todas as informações relevantes e os faz confiar em modelos mentais simplificados, estratégias aproximadas e heurísticas.

Primeiramente as pessoas simplificam as escolhas disponíveis usando heurísticas[15] e só então aplicam sua racionalidade para selecionar a melhor opção entre as restantes. Esse processo pode ou não levar à mesma escolha que o agente econômico racional clássico teria feito (Acquisti *et al,* 2017, p.5).

Existem numerosos exemplos de racionalidade limitada na vida cotidiana. A título de exemplo, ao comprar um determinado produto, não necessariamente a pessoa irá considerar todas as alternativas possíveis que estão disponíveis, como comprar em uma loja diferente, comprar on-line, usar dinheiro, usar um cartão de crédito etc., tampouco as implicações relacionadas a eventual divulgação de seus dados pessoais. Pelo contrário, é possível que o indivíduo simplesmente compre o produto desejado usando qualquer forma de pagamento que lhe seja mais conveniente no momento da compra, além de ser improvável que invista esforços para entender as políticas de privacidade ou termos de serviço de uma loja online que vende o produto almejado; afinal, a maioria dos usuários aceita as políticas sem lê-las (Acquisti *et al,* 2017, p.5).

---

[15] Heurísticas são atalhos mentais ou regras práticas que as pessoas usam para fazer julgamentos e tomar decisões. Eles podem ser úteis para simplificar problemas complexos, mas também podem levar a erros e vieses no pensamento (KAHNEMAN, 2012).

Além do mais, ainda que com acesso a informações completas e poder cognitivo para processá-las exaustivamente, vieses comportamentais podem levar os indivíduos a realizar ações sistematicamente diferentes daquelas previstas pela teoria da escolha racional (Acquisti; Grossklags, 2008, p.364).

Por todos esses motivos, Alessandro Acquisti, Laura Brandimarte e George Loewenstein (2022, p.62) afirmam que as ferramentas tradicionais para a tomada de decisões de privacidade, como escolha e consentimento, já não conseguem fornecer a proteção adequada, de maneira que, em substituição à responsabilidade individual, pode ser necessário lançar mão da intervenção regulatória para equilibrar os interesses dos titulares dos dados ao poder das organizações comerciais e governamentais que detêm os dados.

3 DESIGN, DARK PATTERNS E DADOS PESSOAIS

3.1 O PAPEL DO DESIGN NAS TOMADAS DE DECISÕES DO USUÁRIO

Design é um termo amplo que é aplicado a uma série de coisas, desde objetos, produtos, serviços, sistemas ou mesmo elementos que não envolvem estrutura física, como, por exemplo, regras e procedimentos organizacionais. Tendo isso em conta, as áreas de enfoque do design são as mais diversas possíveis. No presente trabalho utilizar-se-á o termo design no sentido de construção de interfaces de sistemas, de design de interação (*interaction design*), cujo foco é em como as pessoas interagem com a tecnologia (Norman, 2013, p.5).

Diariamente, interage-se com inúmeros produtos digitais, como redes sociais, *sites* e objetos conectados à internet. O uso de tais tecnologias se dá em atividades como entrega de refeições, transporte, comunicações privadas, dentre outras. São interações mediadas por interfaces humano-máquina (*human machine interfaces* – HMI).

Interfaces de usuário são fruto do trabalho conjunto da engenharia, que define sua capacidade de ação e reação, e do design, que determina as representações (visuais, arquitetônicas, verbais etc.) que guiam os usuários em suas interações com as máquinas (CNIL, 2019, p.7).

Interface é "o elemento que estabelece uma conexão física ou lógica entre dois sistemas ou partes de um sistema que não poderiam estar diretamente conectados" (Sawaya, 1999, p.239 *apud* Lemes, 2018, p.39). No ambiente digital, portanto, é a interface gráfica o meio de comunicação entre humano e máquina, mediando a interação das pessoas com dispositivos tecnológicos, como computadores e smartphones etc (Lemes, 2018, p.39).

Para o psicólogo cognitivo Don Norman quando se interage com um produto, é preciso descobrir como ele funciona, o que ele faz e o que é possível de ser fazer com ele. A facilidade com que os usuários conseguem descobrir e compreender as funcionalidades e recursos de um produto, sistema ou interface é o que o autor denomina *discoverability.* Nesse sentido, a interface deve ser de fácil compreensão e manuseio, pois é essencial que os usuários, ao interagirem com uma interface, consigam inferir naturalmente as ações possíveis de se fazer. Para o autor essa "capacidade de descoberta" da interface resulta da aplicação de cinco conceitos psicológicos: *affordances*, *significantes*, *restrições*, *mapeamento* e *feedback*. (Norman, 2013, p.10).

De forma resumida, *affordance* refere-se às possibilidades de interação que o ambiente proporciona ao indivíduo (Norman, 2013, p.11), diz respeito, portanto, às interações potenciais entre uma interface e o usuário. As *significantes*, por sua vez, comunicam onde a ação deve ocorrer (Norman, 2013, p.14), ou seja, sinaliza como operar a interface. Já as *restrições* são as limitações de ações possíveis na interface. Pelo *mapeamento* se estabelece as conexões lógicas entre uma ação e seu efeito no sistema, e por meio dos *feedbacks* o usuário é informado do resultado da ação realizada (CNIL, 2019, p.7).

Nesse contexto, é por meio das interfaces que se apresenta ao usuário os limites e possibilidades de suas ações e escolhas, de maneira que o design da interface pode refletir uma intenção de como uma tecnologia da informação deve funcionar ou ser usada (Hartzog, 2018, p.8).

Richard Thaler e Cass Sunstein denominam "arquitetura de escolha" o ambiente que apresenta o contexto no qual as pessoas podem agir e tomar decisões e como as escolhas são apresentadas a elas (Thaler; Sunstein, 2019, p.11); é por onde design e usuário dialogam (Johnson, 2021, local. 998). A arquitetura de escolha tem como característica não ser neutra; a forma com que o design é construído, independente se de forma deliberada ou não intencional, leva os usuários a tomar determinadas ações e decisões (CMA, 2022, p.3), afinal os usuários respondem aos sinais e opções que a tecnologia lhes oferece. Só é possível clicar nos botões e alternativas que são apresentados. (Hartzog, 2018b, p.8).

Para Hartzog, de maneira geral, o design comunica informações e permite ou impede atividades, podendo atuar como um meio, comunicando-se em nome de designers e usuários, e podendo agir sobre os usuários, restringindo ou capacitando-os de maneiras específicas (Hartzog, 2018b, p.26).

Dessa forma, a depender de como for construído, o design pode literalmente impedir determinadas decisões pelo indivíduo, limitando seu espaço de ação, ou incentivá-lo a tomar determinadas escolhas.

Thaler e Sunstein utilizam o termo *nudge*[16] para se referir a "qualquer aspecto da arquitetura de escolhas capaz de mudar o comportamento das pessoas de forma previsível sem vetar qualquer opção e sem nenhuma mudança significativa em seus incentivos econômicos" (Thaler; Sunstein, 2019, p.14). Por meio do *nudge* o arquiteto de escolha não cria obstáculos às escolhas do indivíduo, apenas o incentiva a tomar determinadas decisões em detrimento de outras (Thaler; Sunstein, 2019, p.14). Dessa forma, o design tem a capacidade de "empurrar" os indivíduos em uma determinada direção, mesmo sem precisar criar obstáculos para tanto.

De acordo com os autores, é impossível que as escolhas das pessoas não sejam influenciadas pela arquitetura. De forma intencional ou não, os indivíduos são orientados em alguma direção (Thaler; Sunstein, 2019, p.19). Logo, cada decisão de design, por mais simples que pareça, pode induzir os usuários a adotarem certos comportamentos. Como as pessoas reagem a sinais e restrições de maneiras previsíveis, o design de tecnologias digitais pode influenciar ou manipular seus usuários para que tomem certas decisões, bem como moldar as percepções e expectativas sobre relacionamentos e riscos. Em outras palavras, se o design facilita algo, o usuário tende a fazê-lo; mas se, por outro lado, dificulta algo, o usuário tende a desistir e buscar uma outra opção (Hartzog, 2018b, p.23).

Ao facilitar ou dificultar uma ação, o design influencia o chamado custo de transação de uma atividade. Custo de transação é um conceito econômico que abrange as despesas envolvidas nas trocas de mercado, porém, ele também pode ser aplicado a qualquer tipo de ação que exija recursos, tal como tempo e esforço; e, com frequência, as decisões das pessoas sobre a realização de determinada tarefa são pautadas na avaliação do tempo que será necessário investir ou do esforço demandado. Mesmo que o custo seja reduzido, pode ser o suficiente para desencorajar certos comportamentos por parte do usuário (Hartzog, 2018b, p.29/30). Por esse motivo, os custos de transação desempenham um papel de enorme importância no design das tecnologias digitais. Um aplicativo ou serviço digital pode ser arquitetado de maneira a encorajar determinadas ações do usuário, e desencorajar outras, conforme o que for mais interessante para o negócio, e não necessariamente respeitando as preferências do usuário.

---

[16] *Nudge* pode ser traduzido como um estímulo, um empurrãozinho ou uma cutucada em determinado sentido.

É o que acontece, por exemplo, com o processo de cancelamento da assinatura do *Amazon Prime*, que foi objeto de análise pelo Conselho Norueguês do Consumidor, o *Forbrukerrådet,* no estudo nomeado "*You can log out, but you can never leave: How Amazon manipulares consumers to keep them subscribed to Amazon Prime*", publicado em 2021. Consoante o verificado na pesquisa, o site foi desenhado de maneira que um usuário consegue fazer sua assinatura do plano *prime* com poucos cliques, porém, caso queira cancelar sua assinatura precisa passar por um processo longo e confuso, marcado pela falta de orientação, por mensagens que enfatizam os benefícios da manutenção da assinatura e um número muito maior de cliques (Forbrukerrådet*,* 2021, p.11). Claramente a intenção da empresa foi aumentar os custos de transação do cancelamento do plano, desestimulando seus usuários a fazerem-no.

Em estudo mais antigo, o *Forbrukerrådet* também verificou que o Facebook desenhou sua interface no sentido de desestimular que seus usuários configurassem sua conta de modo a limitar a coleta e compartilhamento de seus dados pessoais. Diante da vigência do Regulamento Geral de Proteção de Dados europeu, a empresa apresentou aos seus usuários um *pop-up*[17] com dois caminhos a percorrer. O caminho fácil era composto por quatro cliques e consistia em aceitar anúncios personalizados de terceiros e o uso de reconhecimento facial. Por outro lado, os usuários que desejavam limitar a coleta e o uso de dados precisavam realizar treze cliques. Isto é, a empresa aumentou os custos de transação do processo que não lhes era mais interessante, estimulando os usuários a não limitarem a coleta de seus dados (Forbrukerrådet*,* 2018, p.20).

Com efeito, os indivíduos usuários de produtos e serviços online estão sujeitos às escolhas feitas por aqueles que constroem o design das interfaces, até porque a arquitetura de escolha não é algo possível de se evitar (Hartzog, 2018b, p. 52). Todo site e aplicativo tem um design, com diferentes opções de escolhas e linguagem, que, por sua vez, afetam o comportamento do usuário. Para Ari Ezra Waldman, os indivíduos são 'configurados' pelo design das tecnologias que utilizam, as quais podem afetar sua autonomia e privacidade (Waldman, 2018, p.103).

Colocando em perspectiva, diante do efeito que o design causa à percepção do usuário sobre o funcionamento da tecnologia, bem como à sua capacidade de fazer escolhas e proteger seus dados (CNIL, 2019, p.27), pode se dizer que o design exerce um poder sobre as pessoas.

[17] O pop-up é um tipo de janela que aparece "de repente" no navegador ou em um aplicativo, podendo conter, por exemplo, informações e opções de escolha de publicidade.

Para Hartzog, embora as pessoas pensem que são atores autônomos e racionais, elas reagem ao design de maneiras previsíveis, sendo facilmente manipuláveis (Hartzog, 2018b, p.34/35).

Por esse motivo tecnologias são desenhadas com o intuito de estimular o comportamento das pessoas no sentido de compartilhar/divulgar seus dados pessoais, dentre outras coisas. Aliás, no atual contexto em que a economia é movida a dados (*data-driven economy*), a utilização de designs voltados para coletar mais e mais dados é fomentada pelo mercado. Enquanto muitas pessoas podem estar completamente alheias às forças que modulam suas preocupações com a privacidade e proteção de seus dados, as empresas que dependem de informações pessoais para seus negócios sabem muito bem o que estão fazendo (Hartzog, 2018b, p.37).

Como abordado no item 2.3.1 deste trabalho, as preferências e comportamentos dos indivíduos relacionados aos seus dados são muito maleáveis, pois são dependentes do contexto e por conta da incerteza sobre as implicações do compartilhamento de informações pessoais. Logo, as pessoas precisam de muitas pistas sobre o que fazer (Hartzog, 2018b, p.37), e é o design que acaba dando esse direcionamento.

Isso tudo evidencia a natureza limitada e ilusória do controle do indivíduo sobre suas informações, como já discutido anteriormente, uma vez que, em última instância, o exercício desse controle no ambiente online ocorre por meio do design, é mediado pelas opções disponibilizadas ao usuário. Eis o motivo, inclusive, que Ari Waldman rechaça que o comportamento dos usuários no sentido de divulgar suas informações seja visto simplesmente como um possível desinteresse pela privacidade. Para o autor, tendo em conta que o compartilhamento de dados é contextual e dependente tanto da capacidade mental do indivíduo quanto das restrições impostas pelo design da interface, o comportamento adotado pelo usuário apenas reflete uma resposta previsível às maneiras pelas quais as organizações utilizam do design para tirar proveito de suas limitações cognitivas (Waldman, 2020, p.105).

3.2 DARK PATTERNS

3.2.1 Design Patterns

A arquitetura de software abrange as decisões relevantes que envolvem a organização de um sistema de software, incluindo a seleção dos elementos estruturais e suas interfaces, a especificação do comportamento por meio de colaborações entre esses elementos, a composição desses elementos em um subsistema maior e o estilo arquitetônico que orienta essa organização. Em outras palavras, a arquitetura de software é responsável por definir a

estrutura do sistema e suas interações, visando à otimização da sua eficiência, qualidade e facilidade de manutenção (Hoepman, 2014, p.2).

Um elemento fundamental na criação de sistemas de software é a utilização de padrões de design, também conhecidos como *design patterns*. Os *design patterns* são soluções que já foram testadas para problemas recorrentes de design de software. Eles representam soluções generalizadas para problemas que ocorrem de forma reiterada em projetos de software, podendo ser aplicados em diferentes linguagens de programação (Hoepman, 2014, p.3).

Esses padrões surgem da experiência acumulada por programadores e engenheiros de software ao longo do tempo, e são documentados como soluções eficazes para determinados problemas de design. Eles fornecem um conjunto de diretrizes e boas práticas que podem ser aplicadas em diferentes contextos de desenvolvimento de software.

O sucesso dos padrões no campo da engenharia de software foi acompanhado pelo surgimento de novas categorias de padrões, como os *anti patterns* e os *dark patterns*. Enquanto os *design patterns* tradicionais representam soluções estabelecidas e eficientes, os *anti patterns* documentam abordagens a serem evitadas, pois são consideradas más práticas. Os *dark patterns*, por sua vez, são soluções de que visam explorar e enganar os usuários (Bösch *et al.,* 2016, p.238/239).

Em resumo, os *anti patterns* destacam o que não deve ser feito em termos de boas práticas, enquanto os *dark patterns* abordam estratégias que podem ser empregadas de forma prejudicial aos usuários (Bösch *et al.,* 2016, p.239).

3.2.2 *Dark Patterns:* definição

Como mencionado, foi o designer Harry Brignull quem cunhou o termo *dark patterns* para se referir a interfaces elaboradas para enganar os usuários a realizarem determinadas ações. O trabalho de Brignull abriu caminho para uma série de pesquisas acadêmicas que procuraram definir *dark pattern*, o que também se observa em algumas legislações e documentos produzidos por autoridades de defesa do consumidor e proteção de dados pessoais.

Segundo Jamie Luguri e Lior Jacob Strahilevitz, *dark patterns* são interfaces de usuário desenhadas com o intuito de confundir os usuários, dificultar que eles expressem suas preferências reais ou manipular os usuários para que executem determinadas ações. Para os autores, esses padrões normalmente levam os usuários a confiarem na tomada de decisão do

Sistema 1 ao invés de processos mais deliberados do Sistema 2[18], explorando vieses cognitivos (Luguri; Strahilevitz, 2021, p.44).

Para Mathur *et al, dark patterns* "são escolhas de design de interface do usuário que beneficiam um serviço online ao coagir, direcionar ou enganar os usuários a tomar decisões que, se totalmente informados e capazes de selecionar alternativas, eles podem não tomar" (Mathur *et al*, 2019, p.2).

Dando destaque ao seu caráter manipulativo, o Conselho Norueguês do Consumidor descreve *dark patterns* como "técnicas e recursos de design de interface destinados a manipular os usuários" (*Forbrukerrådet* , 2018, p.3).

Quem também propôs um conceito de *dark pattern* foi o Comitê sobre políticas do consumidor da Organização para a Cooperação e Desenvolvimento Econômico (OECD):

> Padrões comerciais obscuros são práticas de negócios que empregam elementos da arquitetura de escolha digital, em particular em interfaces de usuário online, que subvertem ou prejudicam a autonomia, tomada de decisão ou escolha do consumidor. Frequentemente enganam, coagem ou manipulam os consumidores e podem causar danos diretos ou indiretos ao consumidor de várias maneiras, embora possa ser difícil ou impossível medir tal dano em muitos casos (OECD, 2022, p.5, tradução nossa).

A autoridade de proteção de dados francesa, *Comission Nationale Infromatique & Libertés* (CNIL), por sua vez, define *dark patterns* como modelos enganosos criados por plataformas e designers de interfaces de serviços digitais que atuam sobre fenômenos psicológicos específicos do indivíduo, e que afetam a capacidade dos indivíduos de proteger efetivamente seus dados pessoais e fazer escolhas conscientes (CNIL, 2019, p.27).

Dentre as legislações, destaca-se a *California Privacy Rights Act (CPRA),* aprovada em 2020 e considerada a primeira legislação a fornecer uma definição de *dark pattern*. A CPRA conceituou o termo como "uma interface de usuário projetada ou manipulada com o

---

[18] Daniel Kahneman diferencia os modos de pensamento em duas classificações originalmente propostas pelos psicólogos Keith Stanovich e Richard West: Sistema 1 e Sistema 2. O Sistema 1 opera automática e rapidamente, com pouco ou nenhum esforço e nenhuma percepção de controle voluntário, ao passo que o Sistema 2 aloca atenção às atividades mentais laboriosas que o requisitam, incluindo cálculos complexos (Kahneman, 2012, p.29/30). Richard Thaler e Cass Sustein se referem aos Sistemas 1 e 2 como Sistema Automático e Sistema Reflexivo, respectivamente. Segundo os autores, poderia considerar que o Sistema Automático é a reação intuitiva do indivíduo e o Sistema Reflexivo seu pensamento consciente. "A intuição pode ser bastante precisa, mas muitas vezes cometemos erros exatamente por confiar demais no Sistema Automático" (Thaler; Sunstein, 2019, p.29/31)

efeito substancial de subverter ou prejudicar a autonomia do usuário, a tomada de decisões ou escolha, conforme definido em regulamento"[19].

Outro mandamento legal que traz uma definição de *dark patterns* é o recente *Digital Service Act* (DSA) da União Europeia, que estabelece em seu Considerando nº 67 que:

> Os padrões obscuros nas interfaces em linha das plataformas em linha são práticas que distorcem ou prejudicam de forma substancial, intencional ou de facto, a capacidade dos destinatários do serviço de fazerem escolhas ou decisões autónomas e informadas. Estas práticas podem ser utilizadas para persuadir os destinatários do serviço a adotar comportamentos indesejados ou decisões indesejadas que tenham consequências negativas para eles.[20]

Também é oportuno fazer menção à *DETOUR Act* (*Deceptive Experiences To Online Users Reduction Act*), que, embora não prescreva uma definição de *dark patterns*, considera como ilegal que qualquer grande plataforma online "projete, modifique ou manipule uma interface de usuário com o objetivo ou efeito substancial de obscurecer, subverter ou prejudicar a autonomia do usuário, a tomada de decisões ou a escolha de obter consentimento ou dados do usuário"[21].

Percebe-se, portanto, que foram desenvolvidas variadas definições sobre *dark patterns* na academia e em algumas legislações existentes. Arunesh Mathur, Jonathan Mayer e Mihir Kshirsagar (2021, p.3/4) chegaram a identificar dezenove definições diferentes, das quais os autores identificaram quatro principais aspectos, discriminados na tabela (Tabela 1) a seguir:

---

[19] CPRA/ Cal. Civ. Code § 1798.140 (l): "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation. Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140. Acesso em: 13 mai. 2023.

[20] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022R2065. Acesso em: 13 mar. 2023.

[21] SEC. 3. UNFAIR AND DECEPTIVE ACTS AND PRACTICES RELATING TO THE MANIPULATION OF USER INTERFACES.
(a) Conduct Prohibited.—It shall be unlawful for any large online operator—
(1) to design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data. Disponível em: https://www.congress.gov/bill/117th-congress/senate-bill/3330/text. Acesso em: 13 mar. 2023.

Tabela 1 – Classificação de definições de *dark patterns.*

Table 1. A classification of various "dark pattern" definitions in academic literature, law, and policy. Documents are ordered by date.

		Academic Publications														Government Materials			
		Brignull [3]	Conti & Sobiesk [9]	Zagal et al. [62]	Lewis [31]	Bösch et al. [4]	Gray et al. [21]	Mathur et al. [35]	Luguri & Strahilevitz [32]	Lacey & Caudwell [29]	Utz et al. [56]	Westin & Chiasson [59]	Waldman [57]	Day & Stemler [11]	Gray et al. [20]	Maier & Harr [34]	NCC [18]	CNIL [42]	DETOUR Act [58]	CPRA [40]
Characteristics of the User Interface	Coercive							◑							◑					
	Deceptive						●	◑							◑					
	Malicious		●																	
	Misleading					●												●		
	Obnoxious														◑					
	Seductive															●				
	Steering							◑									●			
	Trickery	●											●							
Mechanisms of Effect on Users	Attack users		◑																	
	Confuse users								◑											
	Deceive users									●										
	Exploit users		◑																	
	Manipulate users		◑						◑			●	●							
	Mislead users															●				
	Steer users													●						
	Subvert user intent	●			●	●						●	●	●						
	Subvert user preferences					●		●	◑									●	●	●
	Trick users					●						●				●				
	Undermine user autonomy																		●	●
	Without user consent			●																
	Without user knowledge																	●		
Role of User Interface Designers	Abuse of designer knowledge						●			●		●				●				
	Designer intent		●	●			●		●						●			●	●	●
Benefits and Harms	Benefit to service		●					●			●				●					
	Harm to users			●			●						●				●			

● Required element of "dark pattern" definition ◑ Alternative element of "dark pattern" definition

Fonte: Mathur; Mayer; Kshirsagar (2021).

Como pode ser observado, o primeiro aspecto aborda as características da interface do usuário que podem exercer influência sobre ele. Nesse sentido, alguns conceitos descrevem *dark patterns* como "truques" de design, enquanto outras as descrevem como interfaces "enganosas" e "maliciosas". Outras características também são atreladas à definição de *dark patterns,* como, por exemplo, ser coercitivo, sedutor e desagradável (Mathur; Mayer; Kshirsagar, 2021, p.3).

O segundo aspecto das definições diz respeito ao mecanismo pelo qual as interfaces podem exercer influência sobre os usuários, destacando as diversas formas pelas quais isso ocorre. Algumas definições ressaltam que os *dark patterns* podem subverter a intenção ou as preferências do usuário. Verifica-se, também, definições segundo as quais esses padrões enganam os usuários, minam a sua autonomia, exploram, manipulam, dentre outros mecanismos (Mathur; Mayer; Kshirsagar, 2021, p.4).

O terceiro aspecto das definições de *dark patterns* refere-se ao papel dos responsáveis pela criação do design de interface do usuário. Algumas definições apontam para o abuso do conhecimento a respeito do comportamento humano, ao passo que outras definições afirmam que os designers implantam intencionalmente os *dark patterns* para atingir um objetivo (Mathur; Mayer; Kshirsagar, 2021, p.5).

O quarto e último aspecto identificado acerca das definições de *dark patterns* são os benefícios e danos resultantes de um design de interface de usuário. Algumas definições indicam que um padrão obscuro tem como objetivo beneficiar um serviço online, enquanto outras definições destacam que a utilização de *dark pattern* implica danos aos usuários. (Mathur; Mayer; Kshirsagar, 2021, p.5).

Nesse ponto, cabe apontar que a falta de um consenso sobre a definição de *dark pattern* pode ser um limitador na compreensão, identificação e, consequentemente, no combate dessas práticas enganosas, além de criar lacunas legais e éticas que podem prejudicar os usuários. Contudo, em que pese a variação entre as definições apresentadas, parece acertada a compreensão de que uma das principais características do *dark pattern* é o seu caráter manipulativo. O principal objetivo do design manipulativo é aumentar o lucro do negócio; e isso pode ser feito de diversas formas, como ao fazer com que os consumidores comprem ou continue a comprar um produto ou serviço que, de outra forma, não adquiririam ou adquiririam em menor quantidade; que desembolsem mais dinheiro em uma compra ou tempo em um serviço do que pretendiam; ou forneçam mais dados pessoais do que gostariam. (OECD, 2022, p.12).

Aliás, é justamente por esse motivo que não se pode considerar que os *dark patterns* tenham surgido acidentalmente. Na verdade, o modelo de negócio subjacente configura uma estrutura de incentivos econômicos à criação de interfaces de usuário com boa performance à luz das métricas e parâmetros pertinentes à atividade explorada. Nesse cenário, o mercado pode ser tornar fomentador da utilização dessas práticas, principalmente onde não são claramente proibidas (OECD, 2022, p.13).

Além de manipulativo, para que o design seja considerado *dark pattern* é essencial que ele seja *malicioso* ou *enganoso*. Por malicioso entende-se qualquer design que seja capaz de causar prejuízo ao indivíduo, mesmo que essa não tenha sido a intenção do designer responsável por sua criação (Jarovsky, 2022, p.7).

De mais a mais, é igualmente inquestionável que os *dark patterns* têm a capacidade de afetar o comportamento do usuário, interferindo diretamente na autonomia do indivíduo em seu processo de tomada de decisão.

Nesse sentido, parece acertado que os componentes fundamentais para a caracterização de um padrão enganoso são: a) design com caráter manipulativo; b) que afeta diretamente o processo decisório do usuário; c) que seja capaz de causar prejuízo ao indivíduo; d) aplicado com o intuito de beneficiar o fornecedor do produto/serviço.

Dessa forma, em que pese as definições ventiladas anteriormente, e considerando que a intenção deste trabalho é focar nas práticas de design endereçadas às decisões do indivíduo relacionada aos seus dados pessoais, tomaremos como referência deste trabalho a definição proposta por Luiza Jarovsky, segundo a qual "um *dark pattern* consiste em escolhas de design de interface do usuário que manipulam o processo de tomada de decisão do titular dos dados de forma prejudicial à sua privacidade e benéfica para o provedor de serviços" (Jarovsky, 2022, p.8, tradução nossa).

A autora usa o termo "*escolhas de design de interface do usuário*" para descrever como os *dark patterns* são incorporados no design de um produto ou serviço, seja por meio de um navegador ou aplicativo. Em outras palavras, sempre que o usuário interage com a interface do provedor de serviços, um *dark pattern* pode estar presente. A expressão 'escolhas de design' também é importante porque destaca que, por trás da aparência neutra de um serviço, existem decisões sendo tomadas por organizações e profissionais de design de interface. Essas decisões podem ser benéficas para os negócios, mas também prejudicar os interesses dos usuários. (Jarovsky, 2022, p.8).

O trecho "*que manipulam o processo de tomada de decisão do titular de dados*" denota o uso de táticas ocultas para levar um indivíduo a tomar uma decisão específica, aproveitando-se de suas vulnerabilidades na tomada de decisão. Os *dark patterns* são considerados práticas manipulativas, pois se apoiam em vieses cognitivos para orientar o processo de escolha do titular dos dados na direção pretendida (Jarovsky, 2022, p.9). Isso resulta em uma restrição da sua autodeterminação pessoal.

Ao mencionar "*de forma prejudicial à sua privacidade"*, subentende-se que o design incentiva o compartilhamento de dados para além do necessário ou tem uma influência negativa na tomada de decisão do titular em relação aos seus dados. Os padrões obscuros utilizam vários vieses cognitivos que aumentam a assimetria de informação entre os titulares e agentes de tratamento. Em havendo o objetivo de se coletar mais dados a partir do uso de elementos da interface para induzir uma escolha específica, priva-se o titular de dados da oportunidade de decidir de forma justa sobre seus dados pessoais (Jarovsky, 2022, p.9).

Por fim, por "*benéfica para o provedor de serviços*", entende-se que os *dark patterns* trazem benefícios ao agente de tratamento. Ao manter os titulares de dados desinformados

sobre suas opções em relação aos seus dados, afastá-los da capacidade de monitorar o uso dos seus dados, ao incentivar o compartilhamento excessivo de dados e o tratamento indiscriminado, entre outras coisas, os controladores e seus parceiros são beneficiários dos *dark patterns* (Jarovsky, 2022, p.9/10).

3.2.3 Heurísticas e vieses cognitivos explorados por *dark patterns*

Estudiosos da área de economia comportamental e psicólogos, como Amos Tversky e Daniel Kahneman, têm demonstrado em seus estudos que os indivíduos, ao invés de tomar decisões racionais, tendem a ser influenciados por uma série de vieses cognitivos. Segundo os autores, "as pessoas confiam em heurísticas que reduzem as tarefas complexas de avaliar probabilidades e predizer valores a operações de julgamento mais simples. Em geral, essas heurísticas são bastante úteis, mas às vezes levam a erros graves e sistemáticos" (Tversky; Kahneman, 1974, p.1124).

É o que ocorre no contexto de privacidade, que muitas vezes exige que os usuários avaliem a probabilidade de eventos adversos de segurança ou de proteção a seus dados que são altamente incertos e muitas vezes distantes no futuro. Essas avaliações de probabilidade podem não ser triviais; pelo contrário, podem exigir muito esforço cognitivo por parte do indivíduo, levando-os a se apoiarem em heurísticas (Acquisti *et al*, 2017, p.5).

As heurísticas funcionam como regras gerais utilizadas pelos indivíduos para encurtar o tempo de tomada de decisão[22]; regras estas, no entanto, que podem levar a vieses sistemáticos (Thaler; Sunstein, 2019, p.33) - por sistemático, entenda-se que são efeitos consistentes e previsíveis, e que podem ser explorados pelo design da interface de um site ou aplicativo (Hartzog, 2018b, p.37).

Dentre os inúmeros vieses que podem ser listados aqui (não há uma lista exaustiva), atentar-se-á aos principais vieses que podem ser explorados por *dark patterns* utilizados no design de interfaces de 'escolhas de privacidade'.

3.2.3.1 Viés de ancoragem (anchoring bias)

[22] "Uma heurística é uma estratégia que ignora parte da informação, com o objetivo de tomar decisões com mais rapidez, economia e/ou precisão do que métodos mais complexos." (Gigerenzer; Gaissmaier, 2011, p.454).

O efeito de ancoragem é um viés cognitivo que expressa a tendência do indivíduo de confiar demais na primeira informação que lhe é oferecida (a "âncora") ao tomar decisões[23]. De acordo com Tversky e Kahneman, "as pessoas fazem estimativas partindo de um valor inicial que é ajustado para produzir a resposta final" (Tversky; Kahneman, 1974, p.1128). Essa informação inicial cria um ponto de referência a partir do qual o indivíduo faz ajustes para tomar uma decisão em uma circunstância específica (Acquisti *et al,* 2017, p.7). Ocorre que, geralmente, esses ajustes são insuficientes, surgindo, assim, um viés (Thaler; Sunstein, 2019, p.34).

Um exemplo cotidiano da incidência desse viés seria o cardápio de um restaurante que lista em suas páginas iniciais itens muito caros; o cliente ficará então ancorado pelos valores mais elevados e considerará os valores dos demais itens como inferiores e vantajosos, mesmo que ainda sejam caros quando comparados com os de restaurantes semelhantes (Jarovsky, 2022, p.15).

Esse viés pode ser explorado, por exemplo, na apresentação das opções de privacidade ao titular dos dados em um site. Baseando-se no viés de ancoragem, o design de um site pode apresentar no menu de privacidade uma primeira opção que seja negligente com a proteção dos dados do titular, que implica em um maior compartilhamento de seus dados, e opções adicionais que sejam apenas levemente protetoras, que implica em menor compartilhamento de dados. Nesse cenário, o titular dos dados será "ancorado" pela primeira opção e induzido a considerar as demais opções como protetoras de seus dados pessoais (Jarovsky, 2022, p.15).

3.2.3.2. Efeito bandwagon (bandwagon effect)

O efeito *bandwagon*, ou efeito de adesão, refere-se à tendência dos indivíduos de inferir que certos comportamentos são corretos quando muitas pessoas fazem o mesmo (Konsumentverket, 2021, p.14). Esse viés tem raízes similares ao "pensamento de grupo" e ao "efeito manada", em que o comportamento do indivíduo é alterado por influência do comportamento do coletivo (Jarovsky, 2022, p.16).

No contexto da privacidade, o efeito bandwagon é facilmente observado nas redes sociais. Vez por outra, por exemplo, se torna *trend* no Instagram o compartilhamento de *stories* em que os usuários divulgam suas informações como fotos e dados de idade, altura, signo, dentre outras coisas. Tem-se, portanto, atitudes negligentes em relação à proteção dos

[23] Disponível em: https://www.pon.harvard.edu/daily/negotiation-skills-daily/the-drawbacks-of-goals/. Acesso em: 20 mar. 2023.

dados que ficam em evidência e, por sua vez, influenciam os demais usuários a fazer o mesmo (Jarovsky, 2022, p.16/17).

3.2.3.3. Efeito de contraste (contrast effect)

O efeito de contraste envolve aspectos visuais; em outras palavras, ele explora a relação entre dois objetos (ou dois textos) com o intuito de reduzir a legibilidade ou gerar uma determinada impressão no observador/leitor. Dessa forma, se o designer tem como objetivo que um determinado texto não seja notado ou bem lido, deve aplicar baixo contraste no esquema de cores. Esse efeito também é comumente observado quando se utiliza esquemas de baixo contraste para opções de proteção de privacidade, de maneira a desviar a atenção dos titulares dos dados e reduzir a probabilidade de que eles escolham as opções mais restritivas (Jarovsky, 2022, p.17).

3.2.3.4. Efeito padrão (default effect ou status quo bias)

O efeito padrão, ou viés do *status quo,* expressa a tendência das pessoas se manterem em uma situação atual, ficando inertes e, consequentemente, resistindo à mudança. Para Thaler e Sustein uma das causas desse viés é a falta de atenção. Muitas pessoas adotam o que os autores denominam de heurística do "ah, tanto faz" (Thaler; Sunstein, 2019, p.46).

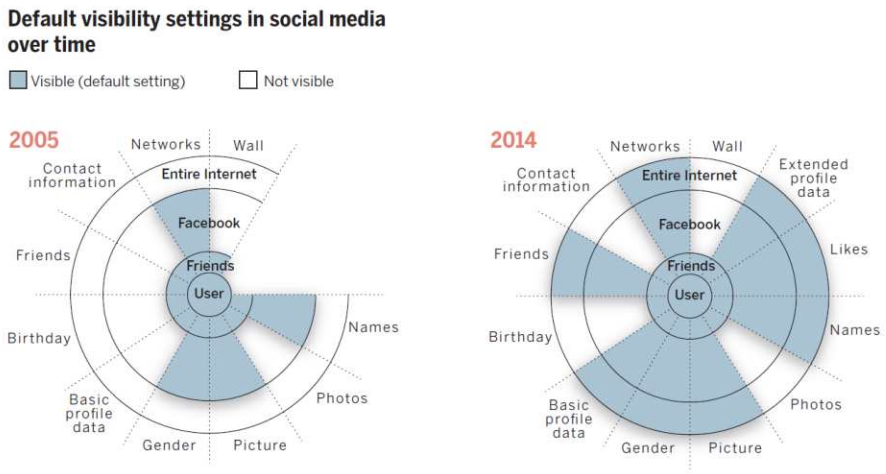
O viés do *status quo* é explorado nos mais diversos contextos, como, por exemplo, o fornecimento de um serviço de forma gratuita por um determinado período, que, se não for cancelado no momento certo, passa a ser cobrado automaticamente – essa prática é comum em serviços como os de assinatura de sites de notícias e de plataformas de *streaming*. A tendência é que o consumidor se mantenha inerte, não cancele o serviço e passe a pagar integralmente por este.

Dessa forma, tem-se as opções-padrão agem como incentivos poderosos (Thaler; Sunstein, 2019, p.47). No campo da proteção de dados, opções-padrão são uma ferramenta importante para induzir a divulgação de informações pelo titular, na medida em que as pessoas geralmente interpretam as configurações padrão como recomendações implícitas por parte do fornecedor (Acquisti; Brandimarte; Lowenstein, 2015, p.512).

Isso pode ser visualizado nas configurações padrão do Facebook relacionadas à visibilidade/divulgação dos dados de seus usuários; com o passar dos anos, foram incluídos vários campos nos perfis de usuários da rede social e as informações passaram a ser

divulgadas para um público cada vez maior, a não ser que o usuário alterasse manualmente as configurações para restringir a exposição de seu perfil (Acquisti; Brandimarte; Lowenstein, 2015, p.513). O gráfico abaixo (Gráfico 1) ilustra a evolução da visibilidade por padrão das informações entre os anos 2005 e 2014:

Gráfico 1 - Configurações de visibilidade padrão no Facebook ao longo do tempo



Fonte: Acquisti; Brandimarte; Lowenstein (2015).

3.2.3.5. Efeito de enquadramento (framing effect)

'O 'efeito de enquadramento' é observado quando nossas decisões são influenciadas pela forma com que as informações são apresentadas (CNIL, 2019, p.16); em outras palavras, as pessoas tomam decisões com o foco na forma como a informação é apresentada ao invés da informação em si[24]. Para Thaler e Sunstein, "o enquadramento funciona porque as pessoas tendem a tomar decisões de maneira desatenta e passiva" (Thaler; Sunstein, 2019, p.48).

Um exemplo de sua manifestação é a comparação de desempenho da publicidade de um alimento com 10% de gordura e outro com 90% sem gordura. O formato que destaca a porcentagem de gordura a menos no produto tende a ser percebida como mais saudável do que o formato que simplesmente informa a porcentagem de gordura presente no produto (Jarovsky, 2002, p.19/20).

Outra forma de ilustrar o enquadramento: um paciente com um problema de saúde questiona seu médico a respeito da possibilidade de fazer uma cirurgia. Na ocasião o médico

[24] Disponível em: https://thedecisionlab.com/biases/framing-effect. Acesso em: 20 mar. 2023.

poderia responder de duas maneiras, que "*de cada 100 pessoas que fazem essa operação, 90 sobrevivem*", ou que "*de cada 100 pessoas que fazem essa operação, 10 morrem".* Embora o conteúdo das duas frases sejam o mesmo, é de se esperar que a primeira mensagem seja mais tranquilizante e que a segunda possa até mesmo fazer com que o paciente desista do tratamento (Thaler; Sunstein, 2019, p.47/48).

No contexto de privacidade, o design de um site ou aplicativo pode enquadrar as opções de forma a destacar os aspectos positivos da coleta dos dados do usuário e encobrir ou ignorar eventuais pontos negativos, provocando o usuário a divulgar seus dados ou escolher uma escolha menos protetiva. Para Ari Waldman esse é o motivo pelo qual empresas de tecnologia explicam suas práticas de uso de dados com linguagem conducente, tais como "se você não permitir cookies, a funcionalidade do site será diminuída" ou "optar pela coleta de dados permitirá funcionalidades novas e mais fáceis" (Waldman, 2020, p.106).

3.2.3.6. Fixação funcional (functional fixedness)

Segundo a Associação Americana de Psicologia "fixação funcional" é a tendência do indivíduo de compreender um objeto apenas em seu uso mais comum (APA, 2023, recurso online)[25]; há uma incapacidade de usar um objeto de maneiras diferentes do que tradicionalmente se destina a ser usado[26].

Aproveitando-se desse viés, pode ser usar na construção de interfaces cores, símbolos ou funções on-line de maneira incomum, confundindo o titular dos dados para selecionar a alternativa menos protetiva a seus dados. Um exemplo simples seria usar um símbolo de cadeado ao lado de uma opção que protege menos a privacidade, induzindo assim o sujeito a erro, na medida em que o titular veria a função do cadeado como um indicativo de proteção aos seus dados (Jarovsky, 2022, p.21).

3.2.3.7. Desconto hiperbólico (hyperbolic discounting)

O termo "desconto hiperbólico" é empregado para descrever a propensão do indivíduo a priorizar recompensas de curto prazo em vez de recompensas futuras, mesmo quando as recompensas imediatas são de menor valor (Konsumentverket, 2021, p.15); há, portanto, uma

[25] Disponível em: https://dictionary.apa.org/functional-fixedness. Acesso em: 20 mar. 2023.
[26] Disponível em: https://thedecisionlab.com/biases/functional-fixedness. Acesso em: 20 mar. 2023.

inclinação do indivíduo a valorizar as consequências imediatas de uma decisão e a subestimar aquelas que ocorrerão no futuro (Waldman, 2020, p.106).

Em um contexto relacionado à privacidade, isso significa que um indivíduo geralmente prefere usar um serviço imediatamente, mesmo que isso envolva riscos ou possíveis impactos em sua privacidade a longo prazo, ao invés de não usar o serviço agora e preservar sua privacidade a longo prazo (Jarovsky, 2022, p.21). Fato é que a divulgação dos dados geralmente traz benefícios imediatos, tais como acesso a um serviço desejado e interação social, ao passo que os riscos dessa divulgação normalmente só serão sentidos muito mais tarde. Nesse cenário, a tendência de supervalorizar as recompensas atuais enquanto desconta inadequadamente o custo dos riscos futuros torna os indivíduos mais dispostos a compartilhar seus dados (Waldman, 2020, p.106).

Exemplo da aplicação desse viés pode ser verificado em estudo da *ENISA* (2012) que identificou que as pessoas preferiam ingressos de cinema um pouco mais baratos, ainda que o ingresso mais barato exigisse maior divulgação de informações pessoais. Já quando os ingressos foram oferecidos pelo mesmo preço, as escolhas dos consumidores mudaram – a companhia de filmes que garantia maior proteção aos dados dos consumidores na venda de ingressos conquistou mais clientes. Os autores concluíram, portanto, que os consumidores estavam descontando os riscos associados à divulgação de informações pessoais, mesmo que diferença de preço dos ingressos fosse pequena (Waldman, 2020, p.106).

3.2.3.8. Aversão à perda

O viés de "aversão à perda" expressa a tendência das pessoas de desgostar mais de uma perda do que gostar de um ganho equivalente (Acquisti *et al*, 2017, p.7). Segundo Thaler e Sustein, "a tristeza de perder algo é duas vezes maior do que a felicidade de ganhar a mesma coisa" (Thaler; Sunstein, 2019, p.44).

Trazendo para o contexto da privacidade, experimentos comportamentais demonstram que as pessoas estão mais dispostas a aceitar dinheiro em troca da divulgação de suas informações pessoais do que estão dispostas a pagar para recuperar o controle sobre as mesmas informações. Em resumo, as pessoas dão maior valor a suas informações pessoais quando se sentem na posse delas – por exemplo, resistem a divulgá-los –, mas quando sentem que já as "perderam", valorizam menos (Acquisti *et al*, 2017, p.8).

3.2.3.9. Viés de otimismo e excesso de confiança

O viés de otimismo é a tendência da pessoa a subestimar as chances de estar sujeita a um evento negativo, ao passo que o excesso de confiança é a tendência do indivíduo de superestimar a precisão de seus julgamentos, resultando em confiança excessiva neles (Acquisti *et al*, 2017, p.9). Ao superestimar sua imunidade individual contra danos, a pessoa pode deixar de tomar medidas sensatas de prevenção (Thaler; Sunstein, 2019, p.44).

No contexto da privacidade, as pessoas podem ter excesso de confiança em sua avaliação de riscos de privacidade ou segurança. Por exemplo, um indivíduo pode estar convencido de que seu software antivírus é totalmente eficaz contra todas as ameaças possíveis, enquanto sua eficácia pode ser substancialmente menor (Acquisti *et al*, 2017, p.9). Como consequência, ele pode tomar isso para si como uma falsa garantia de que comportamentos online negligentes, descuidados e arriscados são inofensivos (Jarovsky, 2022, p.22).

3.2.4 *Dark Patterns:* Taxonomia

No que diz respeito aos diferentes tipos de padrões obscuros existentes, nota-se uma ampla variedade de práticas que se enquadram como tal. A literatura apresenta numerosas taxonomias propostas, as quais, devido à sua própria natureza, dificilmente conseguem abarcar todas as possíveis situações. Essas taxonomias refletem os objetivos dos autores e os critérios adotados por eles, sem contar que o avanço tecnológico contribui para o surgimento contínuo de novos padrões enganosos ao longo do tempo (OECD, 2022, p.11).

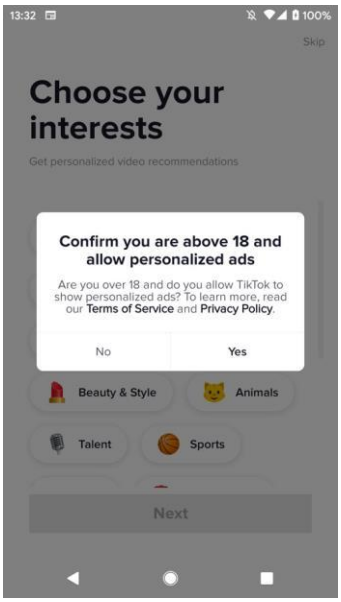
Tendo como base as taxonomias encontradas na literatura, tais como as propostas por Bösch *et al* (2016), Marthur *et al* (2019), Gray *et al* (2018), e Luguri e Strahilevitz (2021), a OCDE apresentou uma lista não exaustiva de categorias de *dark patterns*, lista esta que será tomada como referência neste trabalho. Os padrões obscuros foram divididos nas seguintes categorias: *Forced Action*; *Interface Interference*; *Nagging; Obstruction*; *Sneaking*; *Social Proof*; e *Urgency.*

3.2.4.1 Forced Action (ação forçada)

Os padrões obscuros de ação forçada visam compelir os usuários a realizar ações específicas para obter acesso a determinadas funcionalidades. Isso pode envolver a exigência de cadastro, induzindo a crença de que é necessário, ou a divulgação excessiva de

informações pessoais (OECD, 2022, p.10). Um exemplo desse tipo de prática é conhecido como *bundled consent*, que consiste na obtenção do consentimento de forma agregada a outras requisições ou abrangendo várias finalidades de processamento de dados simultaneamente, sem oferecer uma distinção clara e opção de consentimento separada para cada finalidade específica. Essa prática pode ser ilustrada no processo de inscrição do aplicativo TikTok (Imagem 1), onde a permissão para receber publicidade personalizada é combinada com a confirmação de que o usuário tem mais de dezoito anos de idade.

Imagem 1 – Exemplo de consentimento forçado utilizado pelo Tik Tok.



Fonte: Newsletter “The Privacy Whisperer” da autora Luiza Jarovsky[27]

3.2.4.2 Interface interference (interferência na interface)

Esse tipo de *dark pattern* tem como objetivo privilegiar ações específicas do consumidor que sejam favoráveis ao negócio por meio da manipulação de informações, podendo explorar efeitos de enquadramento, ancoragem ou viés de *status quo*. Exemplos incluem ocultar visualmente informações importantes; a pré-seleção por padrão de opções favoráveis ao negócio (Imagem 2); a atribuição de maior destaque visual a opções favoráveis ao negócio, criando uma falsa hierarquia; o uso intencional de ambiguidade ou perguntas com dupla negação para confundir o usuário; a manipulação do consumidor por meio de

[27] Disponível em: https://www.theprivacywhisperer.com/p/dark-patterns-deceptive-design-in. Acesso em: 03 jul. 2023.

linguagem emotiva ou enquadramento para direcionar uma escolha específica (OECD, 2022, p.10).

Imagem 2 – Exemplo de configuração pré-selecionada que autoriza o tratamento de dados para envio de publicidade.

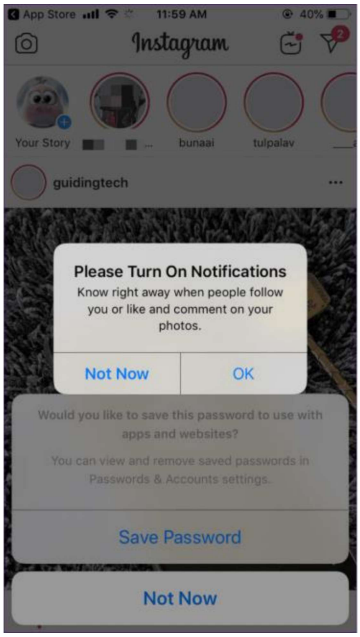
Fonte: Site da Lojas Riachuelo[28]

3.2.4.3 Nagging (insistência/persistência)

Esses padrões envolvem solicitações insistentes ao usuário para que ele realize algo favorável ao negócio, como, por exemplo, ativar notificações (Imagem 3) ou o rastreamento de localização, podendo, portanto, explorar a falta de disposição e tempo do consumidor (OECD, 2022, p.10).

Imagem 3 – Exemplo de *nagging* no Instagram, que solicita ao usuário a ativação de notificações e não oferece a oportunidade de descartar permanentemente a mensagem.

[28] Disponível em: https://www.riachuelo.com.br/cliente/criar-conta. Acesso em: 03 jul. 2023.



Fonte: Brignull *et al* (2023)[29]

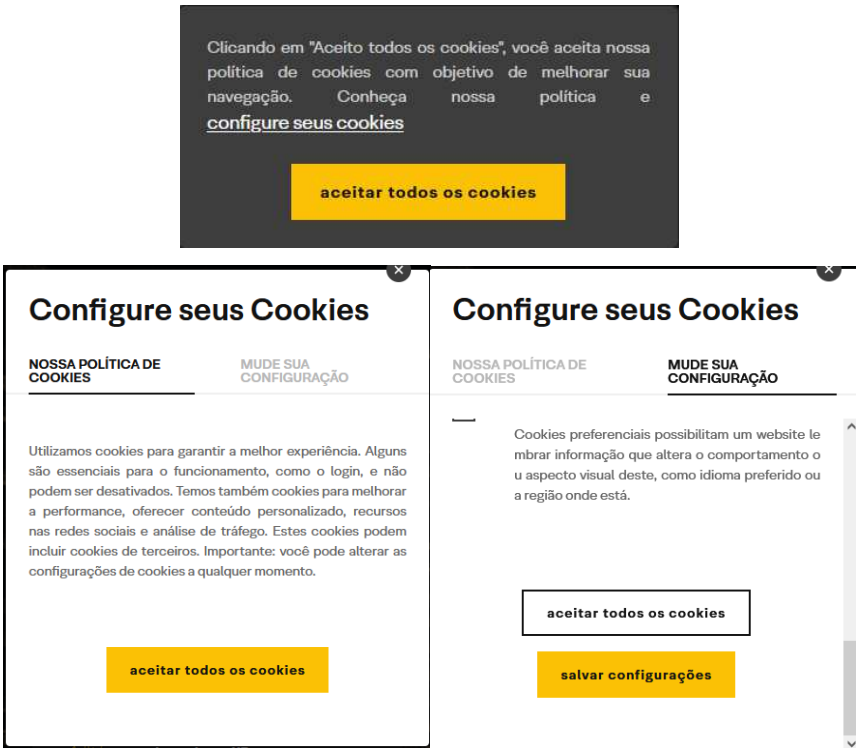
3.2.4.4 Obstruction (obstrução/obstáculo):

Os padrões de obstrução têm como objetivo tornar uma tarefa ou interação mais difícil do que seria necessário, com o objetivo direcionar o indivíduo para realizar uma determinada ação. Exemplo disso é facilitar o processo de inscrição em um serviço ou a adesão a configurações invasivas de privacidade, e, por outro lado, dificultar o cancelamento do serviço ou a opção por configurações que garantam maior proteção aos dados pessoais (OECD, 2022, p.10).

Como ilustração, pode-se mencionar o processo de configurações dos cookies do site da XP Investimentos (Imagem 4). Para aceitar os cookies utilizados na página basta clicar em "Aceitar todos os cookies"; por outro lado, para garantir que apenas os cookies necessários sejam utilizados é necessário clicar em "configure seus cookies", depois clicar em "mude sua configuração", rolar a tela até o fim e clicar em "salvar configurações":

Imagem 4 – Banner de cookies do site XP Investimentos

[29] Disponível em: https://www.deceptive.design/types/nagging. Acesso em: 03 jul. 2023.



Fonte: Site da XP Investimentos[30]

3.2.4.5 *Sneaking* (furtivo/sorrateiro):

Os padrões dessa categoria têm como objetivo ocultar, disfarçar ou atrasar a divulgação de informações relevantes para a tomada de decisão do usuário, especialmente no que diz respeito aos custos. Exemplos desses padrões incluem a inclusão de cobranças não opcionais e significativas ao preço total quando o consumidor está prestes a finalizar uma compra (*drip pricing*); a inclusão de um item no carrinho de compras do consumidor sem o seu consentimento, também conhecido como *sneak into the basket* (Imagem 5); ou a renovação automática de uma compra, inclusive após um período de teste, sem o consentimento explícito do consumidor (OECD, 2022, p.10).

Imagem 5 – Exemplo de *sneaking*, em que um item é inserido automaticamente no carrinho de compras online

[30] Disponível em: https://www.xpi.com.br/. Acesso em: 03 jul. 2023.

(a) Sneak into Basket on avasflowers.net. Despite requesting no greeting cards, one worth $3.99 is automatically added.

Fonte: Mathur *et al* (2019).

3.2.4.6 *Social proof* (prova/evidência social)

Buscam influenciar uma decisão com base na observação do comportamento de outros consumidores. Exemplos incluem notificações sobre as atividades de outros consumidores (Imagem 6) ou depoimentos sobre suas compras recentes, que podem ser falsos (OECD, 2022, p.11).

Imagem 6 – Exemplo de prova social indicando que várias pessoas adicionaram o produto no carrinho nas últimas horas.

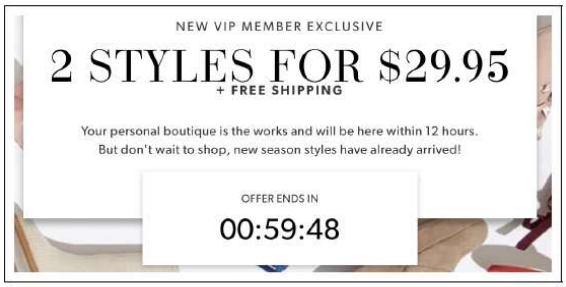
(a) Activity Notification on tkmaxx.com. The message indicates how many people added the product to the cart in the last 72 hours.

Fonte: Mathur *et al* (2019).

3.2.4.7 *Urgency* (urgência)

Padrões de urgência visam impor um limite temporal ou quantitativo, seja real ou fictício, a uma oferta com o intuito de pressionar o consumidor a realizar uma compra, aproveitando-se da heurística da escassez. Exemplos desses padrões incluem exibir mensagens de estoque limitado e alta demanda, ou utilizar um cronômetro de contagem regressiva (Imagem 7) para indicar a iminente expiração de uma oferta ou desconto (OECD, 2022, p.11).

Imagem 7 – Exemplo de cronômetro que indica a expiração de uma oferta, que, na verdade, continua disponível mesmo após o fim do tempo.



(b) Countdown Timer on justfab.com. The offer is available even after the timer expires.

Fonte: Mathur *et al* (2019).

Cada uma das categorias supramencionadas é composta por vários tipos de *dark patterns*, que ainda podem sofrer variações de nomenclatura de acordo com os autores. Convém destacar, ainda, que esses padrões obscuros não são necessariamente utilizados de forma isolada; pelo contrário, é comum que essas técnicas sejam utilizadas em conjunto para aumentar a eficácia da manipulação.

Considerando que a proposta do presente trabalho é dar enfoque às práticas utilizadas no contexto do tratamento de dados pessoais, é oportuno elencar mais exemplos representativos desses *dark patterns*. Assim, tendo como base a compilação oferecida pela OECD (2022, p.53), a tabela a seguir (Tabela 2) apresenta um rol não-exaustivo de padrões obscuros e suas manifestações no âmbito do tratamento de dados pessoais:

Tabela 2 – Tipos de *dark patterns* utilizados em tratamento de dados pessoais.

Categoria	Nome do Dark Pattern	Descrição	Fonte
Forced Action	Forced Registration	Usuário é forçado a se cadastrar ou induzido a acreditar que o cadastro é necessário	Bosch *et al* (2016)
	Forced disclosure/ Privacy Zuckering/ Pressure	O titular enganado ou forçado a compartilhar mais informações pessoais do que o desejado.	Bosch *et al* (2016); Brignull (2010); Jarovsky (2022)
	Impenetrable Wall	Bloquear o acesso a um serviço através de uma barreira de cookies ou criação de conta quando não é necessário para usar o serviço (“take it or leave it"). Nenhuma alternativa sem rastreamento é disponibilizada.	CNIL (2019)
Interface interference	Hidden Information/ Left in the dark	Informações, opções ou ações relevantes para o usuário não são imediatamente acessíveis	Gray et al (2018); EDPB (2022)
	Preselection/ Default sharing	A opção mais invasiva à privacidade do usuário é pré-selecionada por padrão.	Gray et al (2018); Bosch *et al*

			(2016); Brignull (s.d); CNIL (2019)
	Mislead	A utilização de linguagem, formulários e elementos de interface para enganar o titular.	Jarovsky (2022)
	Bad Defaults	As configurações padrão favorecem ou encorajam o compartilhamento de informações pessoais.	Bosch *et al* (2016);
	Framing	As opções são enquadradas de maneiras diferentes a fim de estimular os usuários a fazerem determinadas escolhas.	Forbrukerradet (2018).
	Skipping	A interface é projetada de maneira que os usuários esqueçam ou não pensem sobre todos ou alguns aspectos de proteção de dados.	EDPB (2022)
	Stirring	Utilização de linguagem ou elementos visuais com o intuito de influenciar o estado emocional do titular de modo que o induza a tomar decisões que vão contra seus interesses de proteger seus dados pessoais.	EDPB (2022)
	Wrong Signal	Utilizar um código gráfico "universalmente" compreendido para significar o oposto, criando assim uma confusão para o usuário em relação à escolha que estão fazendo. Por exemplo, adicionar um cadeado a uma interface não especialmente segura.	CNIL (2019)
Nagging	Nagging/ Overloading/ Repetitive Icentive	O usuário é constantemente interrompido com solicitações para fazer algo que pode não ser do seu interesse, como concordar com novos tratamentos ou compartilhar mais dados.	Gray et al (2018); EDPB (2022); CNIL (2019)
Obstruction	Hard to cancel or opt out/ Ease/ Making It Fastiduous to Adjust Confidential Settings	Assimetria entre a facilidade de se cadastrar em um serviço ou autorizar um tratamento de dados e a dificuldade de se descadastrar ou revogar o consentimento/ escolher opções mais protetivas aos dados pessoais.	Brignull (s.d); Forbrukerradet (2018); CNIL (2019)
	Immortal accounts	O provedor de serviços impede que os usuários excluam suas contas e os dados associados.	Bosch *et al* (2016)
	Hinder	Visa atrasar, ocultar ou dificultar que o titular aja com o intuito de proteger seus dados pessoais.	Jarovsky (2022)
	Obfuscating Settings	Criar um processo deliberadamente longo e tedioso para obter as melhores configurações ou torná-las tão refinadas e complicadas que encorajarão o usuário a desistir antes de atingir seu objetivo inicial.	CNIL (2019)
Sneaking	False Continuity	Pedir ao usuário que forneça seu endereço para ler o artigo (título) sem dar um aviso suficientemente claro de que se trata na verdade de uma assinatura de uma *newsletter* (ou com um tamanho de letra tão pequeno que não pode ser lido).	CNIL (2019)
	Camouflaged advertising	A publicidade é disfarçada como outro tipo de conteúdo ou elemento da interface, na	CNIL (2019)

		esperança de que o usuário clique sem saber que se trata de publicidade.	

Fonte: Elaborado pelo autor (2023), inspirado em tabela apresentada pela OECD (2022).

4 A UTILIZAÇÃO DE *DARK PATTERNS* A LUZ DO REGIME DE PROTEÇÃO DE DADOS BRASILEIRO

Como previamente abordado, os *dark patterns* adotam variadas formas e estão presentes em diferentes contextos, representando estratégias amplamente empregadas na configuração das interfaces com as quais os indivíduos interagem rotineiramente. Além disso, é importante ressaltar que tais designs manipulativos têm servido como canais para o tratamento de dados pessoais. Dessa forma, é imperativo que sua utilização seja analisada também sob a égide da legislação nacional de proteção de dados, o que será realizado neste capítulo. Precisamente, a análise será conduzida com base em três pilares: a boa-fé; as hipóteses de tratamento, notadamente o consentimento, e o princípio do *privacy by design.*

4.1 A BOA-FÉ OBJETIVA E DARK PATTERNS

4.1.1 Boa-fé no direito brasileiro: funções e deveres anexos

A expressão "boa-fé" é empregada de diferentes formas no ordenamento jurídico brasileiro, ora como um conceito indeterminado presente em uma regra jurídica, ora como um princípio, ora constituído com acepção objetiva ora subjetiva, embora melhor se qualifique como instituto ou modelo jurídico (Martins-Costa, 2018, local. 880).

Boa-fé é um termo intrinsecamente vago e, portanto, necessita de concretização, o que implica que sua aplicação sempre dependerá do contexto específico. Ou seja, seu significado preciso está vinculado às circunstâncias que determinam o contexto em que será aplicado (Martins-Costa, 2018, local. 905/909).

Segundo as lições de Judith Martins-Costa (2018, local. 916), o agir em conformidade com a boa-fé objetiva efetiva as demandas de integridade, retidão e comportamento leal, essenciais para viabilizar o tráfico negocial apropriado, levando em conta a finalidade e a utilidade do negócio em questão, bem como o campo específico de atuação em que a relação obrigacional é estabelecida, foi estabelecida ou pretende-se estabelecer.

Para a autora a boa-fé objetiva desempenha múltiplas funções no âmbito das relações obrigacionais. Primeiramente, atua como base para a geração de deveres jurídicos, como

cooperação, informação, proteção e consideração das expectativas legítimas do outro contratante. Em segundo lugar, serve como referencial para o exercício das posições jurídicas, corrigindo o conteúdo contratual e regulando o próprio desempenho das partes no contrato. Por fim, a boa-fé objetiva atua como um princípio interpretativo dos negócios jurídicos obrigacionais. Desse modo, a boa-fé objetiva exerce uma função fundamental como orientadora na interpretação dos contratos, como fonte para a harmonização de suas disposições e como critério para a correção de comportamentos contratuais inadequados (Martins-Costa, 2018, local. 929).

Vale ressaltar que, quando aplicado, o princípio da boa-fé é dotado de prescritividade, ou seja, é produtor de normatividade, e, como tal, é capaz de impor condutas, proibições, permissões e estímulos (Martins-Costa, 2018, local. 5361/5467).

A boa-fé objetiva não se baseia na intenção das partes envolvidas na relação jurídica, mas sim na análise objetiva de seus comportamentos. Além de impor deveres às partes, serve como critério para identificar condutas abusivas. Nas palavras de Cláudia Lima Marques:

> [...] a *boa-fé objetiva* é um *standard*, um parâmetro objetivo, genérico, que não está a depender da má-fé subjetiva do fornecedor A ou B, mas de um patamar geral de atuação, do homem médio, do bom pai de família que agiria de maneira normal e razoável naquela situação analisada (...). Boa-fé objetiva significa, portanto, uma atuação refletida, uma atuação refletindo, pensando no outro, no parceiro contratual, respeitando-o, respeitando seus interesses legítimos, suas expectativas razoáveis, seus direitos, agindo com lealdade, sem abuso, sem obstrução, sem causar lesão ou desvantagem excessiva, cooperando para atingir o bom final das obrigações: o cumprimento do objetivo contratual e a realização dos interesses das partes" (Marques *apud* Benjamin; Marques; Bessa, 2021, p.[592]).

Já quando considerado em sua acepção subjetiva, a boa-fé refere-se a um estado psicológico reconhecido em uma pessoa e que constitui um requisito presente no contexto fático de certas normas jurídicas, influenciando a produção de efeitos jurídicos (Miragem, 2016, p.145); caracteriza-se pelo desconhecimento do indivíduo de estar a causar qualquer lesão ou violação aos direitos de outrem (Martins-Costa, 2018, local. 5361), se contrapõe à má-fé.

No contexto brasileiro, é relevante mencionar que o princípio da boa-fé objetiva já estava previsto no artigo 131, inciso I[31], do Código Comercial de 1850 e, de forma específica,

[31] Art. 131 - Sendo necessário interpretar as cláusulas do contrato, a interpretação, além das regras sobreditas, será regulada sobre as seguintes bases:
1 - a inteligência simples e adequada, que for mais conforme à boa fé, e ao verdadeiro espírito e natureza do contrato, deverá sempre prevalecer à rigorosa e restrita significação das palavras;

no artigo 1.443 do Código Civil de 1916, que tratava do contrato de seguro[32]. Contudo, até a promulgação do Código de Defesa do Consumidor, a boa-fé era abordada pelos tribunais brasileiros majoritariamente em sua dimensão subjetiva[33]. No entanto, ao longo dos séculos XIX e XX, o rápido desenvolvimento do capitalismo e o advento de uma sociedade de massas trouxe à margem a utilização práticas abusivas por parte de agentes econômicos em relação a contratantes mais vulneráveis. Diante da necessidade de combater esses abusos, surgiram diversas iniciativas, dentre elas a promulgação do CDC (Tepedino; Scheireber, 2003, p.139/140).

Com o CDC a boa-fé objetiva foi expressamente prevista como um dos princípios norteadores da Política Nacional de Relações de Consumo:

> Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:
> (...)
> III - harmonização dos interesses dos participantes das relações de consumo e compatibilização da proteção do consumidor com a necessidade de desenvolvimento econômico e tecnológico, de modo a viabilizar os princípios nos quais se funda a ordem econômica (art. 170, da Constituição Federal), sempre com base na boa-fé e equilíbrio nas relações entre consumidores e fornecedores;

A boa-fé também é encontrada no art. 51, que dispõe que obrigações incompatíveis com a boa-fé serão consideradas nulas:

> Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que:
> (...)
> IV - estabeleçam obrigações consideradas iníquas, abusivas, que coloquem o consumidor em desvantagem exagerada, ou sejam incompatíveis com a boa-fé ou a equidade;

Como pode ser observado, as normas em questão não têm como base a boa-fé subjetiva, ou seja, o estado de consciência do fornecedor ou do consumidor, mas sim em uma

---

(...)

[32] Art. 1.443. O segurado e o segurador são obrigados a observar no contrato a mais estrita boa-fé e veracidade, tanto em relação ao objeto, quanto às circunstâncias e declarações a ele referentes.

[33] O Código Civil de 1916 também adotava essa perspectiva. Em seu art. 490 previa que: "É de boa-fé a posse, se o possuidor ignora o vício, ou o obstáculo que lhe impede da aquisição da coisa, ou do direito possuído.".

concepção de boa-fé que se desvincula das intenções íntimas do sujeito. Essa concepção exige comportamentos objetivamente adequados aos princípios de lealdade, honestidade e colaboração para alcançar os objetivos estabelecidos em cada relação obrigacional (Tepedino; Schreiber, 2003, p.141).

Posteriormente, o Código Civil de 2002 também passou a prever expressamente a aplicação do princípio da boa-fé objetiva. No art. 113 a boa-fé é prevista como fonte de interpretação dos negócios jurídicos; no art. 187 é considerada como critério de aferição de licitude de atos praticados dentro do contexto negocial e no art. 422 é posto como cláusula geral dos contratos, servindo à sua integração:

> Art. 113. Os negócios jurídicos devem ser interpretados conforme a boa-fé e os usos do lugar de sua celebração.
>
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.
>
> Art. 422. Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé.

A boa-fé como *standard* jurídico também está prevista na LGPD, que dispõe expressamente em seu artigo 6º que "os tratamentos de dados pessoais deverão observar a boa-fé", o que implica dizer, em suma, que os agentes de tratamento de dados, ao processar dados pessoais em suas atividades, deverão agir de forma leal com o titular dos dados, agir com correção, sem abusos, e levando em consideração os interesses legítimos do titular. Essa inserção no texto da LGPD também reforça que, embora a relação obrigacional seja o campo em que a aplicação da boa-fé é mais proeminente, esse princípio possui natureza abrangente, estendendo-se a todas as relações jurídicas presentes na sociedade (Pereira, 2013, p.23).

Em suma, pode-se dizer que o princípio da boa-fé exerce três funções fundamentais: 1) diretriz ou critério interpretativo; 2) criador de deveres jurídicos adicionais; e 3) limitador do exercício de direitos subjetivos.

Como diretriz hermenêutica, a boa-fé objetiva orienta que, diante de várias opções interpretativas, as relações jurídicas devem ser entendidas em consonância com uma esperada lealdade e honestidade das partes envolvidas (Benjamin; Marques; Bessa, 2021, p.[593]). Dessa forma, evita-se qualquer interpretação que possa atribuir a uma cláusula contratual, p.ex, uma conotação maliciosa ou que busque de alguma forma enganar ou prejudicar uma das partes em benefício da outra (Tepedino; Schreiber, 2003, p.145).

No que diz respeito à função de criação de deveres anexos, Bruno Miragem (2016, p.146) destaca que além dos deveres principais da relação obrigacional, também serão observados deveres anexos e laterais, que não decorrem diretamente da obrigação principal, ou seja, independem da vontade das partes envolvidas, mas visam atender aos seus interesses gerais. Entre esses deveres encontram-se os deveres de cuidado, previdência, correção, segurança, cooperação e informação.

A propósito, é oportuno mencionar que tais deveres se relacionam diretamente com os demais princípios previstos nos incisos do art. 6º da LGPD, aplicáveis aos tratamentos de dados de dados pessoais. A título de exemplo, os princípios da finalidade e necessidade se conectam ao dever de correção; os princípios da transparência e livre acesso estão associados aos deveres de informação e colaboração, assim como o princípio da segurança está ligado aos deveres de segurança e cuidado e o princípio da prevenção pode ser associado ao dever de previdência.

No que tange à terceira função, a de limitadora do exercício de direitos subjetivos, a boa-fé visa "impedir o exercício manifestamente desleal, incoerente, imoderado ou irregular de direitos subjetivos, formativos, faculdades e posições jurídicas" (Martins-Costa, 2018, local. 11733); serve, portanto, como parâmetro para valorar a conduta das partes e identificar a prática de abusos de direito (Benjamin; Marques; Bessa, 2021, p.[595]).

Por fim, a conduta pautada na boa-fé deve ser observada mesmo antes da formalização de uma determinada relação e, igualmente, perdurar além do momento em que formalmente se encerra (Miragem, 2016, p.146).

4.1.2 A boa-fé objetiva como obstáculo à utilização de *dark patterns*

Conforme delineado anteriormente, a relação entre o titular de dados e o responsável pelo tratamento de dados é marcada principalmente pela assimetria informacional entre as partes, o que se retira do confronto entre o poderio de processamento de informações do agente de tratamento e as limitações técnicas e cognitivas do titular. Essa assimetria coloca o titular em uma posição passiva, com poucas condições de avaliar os riscos decorrentes do tratamento de seus dados e, consequente, de tomar decisões no sentido de protegê-los.

Nesse cenário, o princípio da boa-fé desponta como ferramenta para reduzir esse desequilíbrio existente entre as partes. Como assinalado, o papel primordial da boa-fé como *standard* jurídico é direcionar os comportamentos aos valores ético-jurídicos da probidade, honestidade, lealdade e da consideração às legítimas expectativas do outro (Martins-Costa,

2018, local. 5416/5423), direcionamento esse que vai permear todas as fases do tratamento de dados, ou seja, o pré-tratamento, o tratamento propriamente dito e o período posterior ao seu término. Isso implica dizer que já na construção da interface de um site ou aplicativo, que será o meio pelo qual o tratamento de dados será realizado, o agente de tratamento deve agir de maneira proba e se abster de utilizar padrões que visam manipular os usuários e que possuam o potencial de lhes causar prejuízos. Em verdade, mais do que evitar a utilização de padrões enganosos, deve-se optar pela criação de um design transparente, colaborativo e centrado na pessoa.

Segundo Don Norman, o design centrado na pessoa, ou no ser humano (*human-centered design – HCD*) é:

> "[...] uma abordagem que coloca as necessidades humanas, capacidades e comportamento em primeiro lugar, para então projetar de forma a acomodar essas necessidades, capacidades e formas de comportamento. Um bom design começa com uma compreensão da psicologia e da tecnologia. Um bom design requer uma boa comunicação, especialmente da máquina para a pessoa, indicando quais ações são possíveis, o que está acontecendo e o que está prestes a acontecer" (Norman, 2013, p.8, tradução nossa).

Para o autor muitos dos sistemas, procedimentos e dispositivos atuais estão focados na tecnologia, desenvolvidos em torno das habilidades tecnológicas, com as pessoas sendo chamadas para preencher as lacunas que a tecnologia não consegue abranger. Uma abordagem centrada nas pessoas busca reverter essa situação, priorizando as necessidades e aptidões humanas (Norman, 2019, recurso online).

Essa perspectiva é coerente com a aplicação do *privacy by design*, previsto no art. 46, §2º, da LGPD, princípio segundo o qual a privacidade deve ser considerada desde a fase de concepção de produtos e serviços, ou seja, desde a criação da arquitetura de um sistema, da construção de uma interface. Igualmente, é compatível com a função restritiva da boa-fé, a qual impede que o responsável pelo tratamento dos dados abuse de sua posição jurídica privilegiada em detrimento do titular dos dados, agindo de maneira desleal. Como visto, há um desequilíbrio de poder premente entre agente de tratamento e titular. É muito difícil para o indivíduo acompanhar a complexidade que o tratamento de dados em meios digitais pode alcançar, de modo que o responsável pelo tratamento deve ter postura de colaboração, a fim de reduzir essa disparidade, evitando se aproveitar da assimetria pré-existente.

Segundo Judith Martins-Costa, dentre as funções exercidas pela boa-fé, está a de aumentar a carga dos deveres informativos do fornecedor justamente com o objetivo de

minimizar a vulnerabilidade do titular consumidor (Martins-Costa, 2018, local. 6175). Desse modo, o responsável pelo tratamento dos dados não pode se limitar a fornecer as informações básicas a respeito do tratamento de dados perpetrado, mas tem o dever de garantir que as informações disponibilizadas sejam efetivamente compreendidas pelo titular, isso porque "a transparência é um conceito eminentemente voltado para os usuários e não para os aspectos jurídicos" (CNIL, 2019, p.40, tradução nossa). Nesse sentido, "a qualidade, acessibilidade e inteligibilidade da informação são tão importantes quanto o conteúdo formal da informação fornecida às pessoas relevantes" (CNIL, 2019, p.40, tradução nossa).

Nesse ponto, vale dizer que o dever de colaboração decorrente da boa-fé impõe uma conduta mais proativa por parte do responsável pelo tratamento. Logo, parece não ser suficiente a simples disponibilização de um aviso/política de privacidade no site ou aplicativo, mas que informações também sejam fornecidas ao longo de toda jornada do usuário no ambiente digital – por exemplo, por meio de feedback, que consiste numa abordagem de design de interação que comunica à pessoa o resultado imediato de uma ação realizada, utilizando mensagens ou indicadores visuais.

Além de reforçar o dever de transparência, o princípio da boa-fé amplifica a solidez dos demais princípios contidos nos diferentes incisos do artigo 6º da LGPD. Agir de maneira honesta e leal com o titular implica, de igual forma, em assegurar que os dados pessoais sejam manejados unicamente para fins específicos, que apenas os dados essenciais para esses propósitos sejam utilizados, que medidas de segurança adequadas sejam implementadas para resguardar os dados sob sua tutela, que os direitos dos titulares sejam respeitados e atendidos devidamente, e que, ao término do tratamento, haja a devida eliminação ou anonimização dos dados. Como mencionado no tópico anterior, os deveres anexos da boa-fé estão intrinsecamente conectados aos demais princípios do art. 6º, de maneira que a violação de um deles acaba por também implicar na transgressão do princípio da boa-fé.

Acrescenta-se, também, que ao utilizar um site ou aplicativo, o titular não tem a expectativa de ser manipulado a tomar uma decisão que não seja do seu interesse; ao contrário, sua expectativa é de que seus direitos sejam respeitados e que o responsável pelo tratamento dos dados forneça as condições necessárias para que ele possa tomar decisões de forma informada e consciente.

Fazendo um paralelo ao GPDR, a boa-fé vai exercer papel similar ao do princípio da justiça/equidade (*fairness*), que, segundo Malgieri, para além da legalidade dos tratamentos, leva em conta as expectativas dos indivíduos, os efeitos do tratamento sobre os titulares e os

interesses das partes envolvidas, e tem com o objetivo prevenir e equilibrar relações assimétricas (Malgieri, 2020).

A este respeito, o *Competition and Markets Authority* (CMA) do Reino Unido, ao examinar a configuração de estruturas de escolha e a disparidade de informação entre plataformas e consumidores, propôs a incorporação de um dever de *fairness by design*, em complemento ao princípio do *privacy by design,* com o intuito de assegurar que as opções e os padrões disponibilizados por plataformas online sejam apresentados de maneira a facilitar a tomada de decisão esclarecida do consumidor acerca da utilização de seus dados pessoais (CMA, 2020, p.34). Conforme a orientação da CMA, as plataformas devem tratar os usuários de maneira justa e imparcial, seguindo três preceitos: a) *acessibilidade*, assegurando que informações e alternativas sejam facilmente compreensíveis e localizáveis, com processos de interação descomplicados; b) *equilíbrio*, garantindo que informações e alternativas sejam apresentadas de modo imparcial, permitindo que os usuários desenvolvam suas próprias perspectivas; e c) *consistência e capacitação*, permitindo aos usuários realizar escolhas conforme suas intenções atuais e respeitando essas escolhas, incluindo a opção de alterar suas decisões posteriormente (CMA, 2020, p.41).

Depreende-se, portanto, que a boa-fé vai diretamente de encontro aos propósitos dos denominados *dark patterns* (Tabela 3). Enquanto a primeira visa promover a confiança e equilíbrio nas interações entre titular de dados e agente de tratamento, por meio dos padrões obscuros as organizações visam reforçar e se aproveitar do desequilíbrio existente entre as partes.

Tabela 3 – Comparativo entre os deveres de conduta decorrentes do princípio da boa-fé objetiva e os propósitos dos *dark patterns*.

Boa-fé objetiva	***Dark Patterns***
Agir com lealdade e honestidade.	Manipular, enganar.
Colaborar com o usuário para que consiga tomar decisões informadas e conscientes.	Induzir o titular a tomar decisões que não tomaria se tivesse acesso a todas as informações necessárias.
Transparência	Falta de clareza; opacidade
Minimizar a assimetria informacional entre titular e agente de tratamento.	Explorar a assimetria informacional entre titular e agente de tratamento.
Design centrado na pessoa.	Design centrado exclusivamente nos

	interesses da organização.

Fonte: Elaborado pelo autor (2023).

4.2 *DARK PATTERNS* E CONSENTIMENTO

Na gestão dos dados pessoais em uma organização, geralmente existem quatro etapas distintas que são a coleta, o armazenamento, o processamento e o descarte dos dados. No que tange aos *dark patterns*, sua aplicação é mais frequentemente observada durante a fase de coleta de dados. Nesse sentido, a principal hipótese de tratamento de dados prevista na LGPD que pode ser afetada pelos *dark patterns* é o consentimento do titular de dados pessoais. Isso porque a modalidade de tratamento de dados baseada no consentimento do titular está diretamente ligada à capacidade do titular de tomar decisões sobre a coleta e o uso de suas informações pessoais (Jarovsky, 2022, p.33/34).

A LGPD prevê em seu artigo 5º, inciso XII, que consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

O adjetivo *livre* implica uma escolha real por parte do titular, ou seja, que o titular tomou uma decisão sem ter sido pressionado ou influenciado de forma manipulativa por terceiros. O qualificador "livre" está intimamente relacionado ao grau de poder que o titular de dados possui em relação ao tratamento de suas informações pessoais. Deve-se avaliar o poder de barganha do cidadão, levando em conta as opções disponíveis em relação ao tipo de dados coletados e seus possíveis usos (Bioni, 2019, p.197), de modo que qualquer forma de pressão ou influência inadequada exercida sobre o titular dos dados, independentemente de como se manifeste, que o impeça de exercer seu livre arbítrio, resultará na invalidade do consentimento (EDPB, 2020b, p.6).

Desse modo, uma arquitetura de escolha construída com padrões de design que compelem o titular a consentir com a coleta de seus dados, afastando, portanto, a autonomia da manifestação de vontade do usuário, torna o tratamento do dado ilegítimo. Um exemplo disso é quando o consentimento é vinculado a um contrato e/ou utilizado para finalidades agrupadas (*bundled consent*) – a exemplo da Imagem 1 –, o que tira a possibilidade do titular manifestar sua vontade acerca de cada uma das finalidades apresentadas.

Por *informado* entende-se que, antes de concordar com o tratamento de seus dados, o titular precisa ser devidamente instruído acerca da finalidade para a qual os seus dados serão utilizados; com quem serão compartilhados, sobre a possibilidade de revogação do

consentimento, dentre outros pontos. Além disso, a informação deve ser ostensiva e em linguagem clara. A informação deve preencher o vazio da assimetria informacional; e, ainda que não leve o titular ao patamar informativo do agente de tratamento, deve fornecer um conteúdo em quantidade e qualidade suficiente para que o titular consiga compreender adequadamente o contexto do tratamento e tomar uma decisão mais consciente (Bioni, 2019, p.192/193).

Nesse cenário, uma interface que apresenta informações insuficientes (ou excessivas[34]), de forma esparsa ou que emprega linguagem ambígua e/ou distorce fatos com o objetivo de induzir o titular dos dados a conceder autorização para a coleta de suas informações compromete o caráter informado do consentimento, e contraria o princípio da transparência estabelecido na LGPD.

O consentimento também requer que a manifestação de vontade do titular seja *inequívoca*, ou seja, que sua intenção seja claramente expressa por meio de uma ação afirmativa. A qualificação do consentimento como inequívoco dependerá da extensão e da qualidade da interação realizada pelo usuário (Bioni, 2019, p.200). Nesse sentido, a utilização de *checkboxes* pré-selecionados que autorizam o tratamento de dados pessoais, por exemplo, não configura um consentimento inequívoco, uma vez que não depende de uma ação ativa por parte do titular, mas sim de sua inação.

Por fim, para ser válido o consentimento precisa ser destinado a uma finalidade determinada. O consentimento deve ser direcionado, portanto, para um propósito legítimo, específico e explícito. Assim sendo, a apresentação da finalidade de maneira que não seja evidente ou de forma genérica, como, por exemplo, a conhecida "para melhoria da sua experiência", torna o consentimento inválido.

Tem-se, portanto, que a autorização do titular obtida por meio de um *dark pattern* não configura consentimento. Inclusive, essa incompatibilidade pode ser depreendida da interpretação do previsto no do §1º do art. 9º da LGPD, segundo o qual o consentimento será considerado nulo caso as informações fornecidas ao titular tenham conteúdo "enganoso" ou "abusivo" – características que podem ser atreladas aos padrões obscuros – ou não sejam transparentes:

> Art. 9º. (...)

[34] "(...) dada a racionalidade limitada (*bounded rationality*) do ser humano, o excesso de informação também desinforma (*overloaded information*)." (BIONI, 2019, p.193)

> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

A título comparativo, a legislação de proteção de dados da California (CCPA) prevê expressamente que a utilização de *dark patterns* impede a constituição do consentimento:

> Consentimento significa qualquer indicação livre, específica, informada e inequívoca dos desejos do consumidor, pela qual o consumidor, ou o responsável legal do consumidor, uma pessoa que detém poder de procuração, ou uma pessoa atuando como tutor para o consumidor, incluindo por meio de uma declaração ou de uma ação afirmativa clara, expressa concordância com o processamento de informações pessoais relacionadas ao consumidor para um propósito particular definido de forma restrita. A aceitação de termos de uso gerais ou amplos, ou documento similar, que contenha descrições de processamento de informações pessoais juntamente com outras informações não relacionadas, não constitui consentimento. Passar o mouse sobre, silenciar, pausar ou fechar um determinado conteúdo não constitui consentimento. Da mesma forma, **um acordo obtido por meio de padrões obscuros (dark patterns) não constitui consentimento**[35]. (tradução nossa, grifo nosso).

Como mencionado, o consentimento é a principal hipótese de tratamento atingida pelos *dark patterns*, mas não a única. É plenamente possível, por exemplo, que esses padrões sejam utilizados dentro de um contexto de uma execução de contrato, em que o fornecedor de um serviço lance mão de padrões para esconder informações relevantes do titular, criar obstáculos para determinadas ações ou mesmo induzir determinada manifestação de vontade do indivíduo – manifestação essa que não se confunde com consentimento.

Exemplo disso é o ocorrido com a empresa Discord Inc., que recentemente foi sancionada pela autoridade de proteção de dados francesa por problemas no design de sua aplicação. De acordo com o CNIL, na versão do aplicativo para Microsoft Windows havia um "X" no canto superior direito que não fechava efetivamente o programa, como era de se

---

[35] "(h) "Consent" means any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose. Acceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agreement obtained through use of dark patterns does not constitute consent." Cal. Civ. Code § 1798.140(h). Disponível em: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>. Acesso em: 10 jul. 2023.

esperar pelo usuário, mas apenas o colocava em segundo plano, o que não era informado ao usuário e permitia, assim, a continuidade do tratamento de dados pessoais[36]. Ou seja, o design da aplicação foi desenhado de modo a favorecer a coleta de dados dos usuários mesmo quando dava a entender ao usuário que isso não ocorria, violando, assim, o princípio da transparência. A propósito, segundo a política de privacidade do Discord[37], o processamento de imagens e áudios em chamadas se dá com o objetivo de fornecer os serviços ao usuário, para cumprir o contrato com o titular.

Outro exemplo de hipótese de tratamento que pode ser afetada pela utilização de padrões obscuros é o legítimo interesse. É o que se retira do recente estudo de Kiy *et al* (2023). Analisando avisos de consentimento, *cookie banners* e *cookies pop-ups* de dez mil sites, os autores identificaram uma série de design enganosos nas situações em que o legítimo interesse estava incluso nos "avisos de privacidade" em questão. Dentre as práticas enganosas assinaladas pelos pesquisadores, cita-se a ausência de opção que permitia ao titular se opor a todos os tratamentos baseados em interesses legítimos de uma só vez, sendo preciso, ao invés disso, que os usuários promovessem o direito à oposição de cada tratamento individualmente; a criação de obstáculos à oposição pelo titular, através, por exemplo, de direcionamento dos usuários à política de privacidade ou ao site do fornecedor terceirizado para se conseguir opor ao processamento; e a utilização de explicações ruins ou vagas sobre o significado de legítimo interesse, sem contar os casos em que o termo foi utilizado sem estar acompanhado de qualquer explanação (Kiy *et al*, 2023, p.[6]).

4.3 DARK PATTERNS E *PRIVACY BY DESIGN*

Desenvolvido nos anos 90 por Ann Cavoukian, o conceito de *privacy by design* (*PbD*) foi criado como uma resposta aos crescentes efeitos sistêmicos das tecnologias de informação e comunicação e dos sistemas de dados em rede em larga escala. Seu objetivo principal é assegurar a privacidade e proporcionar controle pessoal sobre as informações individuais, ao mesmo tempo em que oferece às organizações uma vantagem competitiva sustentável (Cavoukian, 2011, p.[1]).

Para Bioni, *PbD* "é a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles ser embarcados com tecnologias que

[36] Disponível em: https://www.cnil.fr/en/discord-inc-fined-800-000-euros. Acesso em: 30 mai. 2023.
[37] Disponível em: https://discord.com/privacy#4. Acesso em: 28 jun. 2023.

facilitem o controle e a proteção das informações pessoais" (Bioni, 2019, p.176). No âmbito do desenvolvimento de sistemas de tecnologia da informação, o conceito de *PbD* estabelece que a proteção da privacidade deve ser considerada um requisito essencial do sistema, a ser abordado de forma equivalente a qualquer outro requisito funcional (Hoepman, 2014, p.1).

A concepção de *Privacy by Design* foi construída com base em sete princípios fundamentais (Cavoukian, 2011, p.[2]):

1) *Proativo, não reativo; preventivo, não reparador*: antecipar e prevenir eventos invasivos à privacidade antes que ocorram, adotando uma postura pró-ativa ao invés de reativa.
2) *Privacidade como padrão* (*privacy by default*): assegurar que os dados pessoais sejam automaticamente protegidos em todos os sistemas de tecnologia da informação e práticas comerciais, sem que os usuários precisem tomar medidas adicionais para garantir sua privacidade.
3) *Privacidade incorporada ao design*: incluir a privacidade como um elemento intrínseco ao projeto e à arquitetura dos sistemas de tecnologia da informação e às práticas comerciais, garantindo que a proteção dos dados pessoais seja considerada desde o início;
4) *Funcionalidade total*: buscar acomodar de forma harmoniosa todos os interesses e objetivos legítimos envolvidos, promovendo soluções que beneficiem todas as partes interessadas;
5) *Segurança de ponta a ponta*: assegurar a segurança dos dados pessoais durante todo o ciclo de vida, desde o armazenamento até a destruição segura, protegendo-os contra acesso não autorizado e garantindo sua integridade;
6) *Visibilidade e transparência*: fornecer garantias a todas as partes interessadas de que as práticas comerciais e as tecnologias estão operando de acordo com as promessas e objetivos declarados, promovendo a transparência em relação ao uso e proteção dos dados pessoais.
7) *Respeito à privacidade do usuário*: colocar os interesses e direitos dos titulares de dados em primeiro plano, oferecendo medidas como padrões de privacidade protetivos, avisos adequados e opções de fácil utilização.

Por meio da implementação do *PbD*, torna-se necessário aplicar medidas de proteção dos dados do titular desde o estágio inicial do desenvolvimento de um produto ou serviço. Portanto, é esperado que sites, aplicativos e sistemas em geral que lidem com dados pessoais

adotem, por padrão, configurações de privacidade altamente restritivas. Nesse contexto, eventual redução da proteção conferida aos dados do usuário deve exigir uma ação proativa por parte dele. Em outras palavras, a opção oferecida ao titular usuário deve ser a de limitar a proteção de seus dados, na medida em que o padrão adotado deve ser o de proporcionar a máxima proteção possível (Lemos; Branco, 2021, p.463).

Em 2012 o *privacy by design* foi reconhecido pelo *US Federal Trade Comission* (FTC) como uma prática para proteger a privacidade online (FPF, 2023, p. 5). Posteriormente, o GDPR incorporou o conceito de *privacy by design* e *privacy by default* em seu art. 25[38], que na versão em português são denominados "proteção de dados desde a concepção e por defeito", estabelecendo que as medidas técnicas e organizacionais de proteção de dados devem ser aplicadas tanto no momento de definição dos meios de tratamento, como no momento do próprio tratamento:

> Artigo 25º
> **Proteção de dados desde a concepção e por defeito**
>
> 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
> 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.
> [...]

De maneira análoga, a LGPD incorporou à sua redação o conceito de *privacy by design*. Dentro do capítulo de "Da Segurança e das Boas Práticas", o art. 46 prevê em seu *caput* que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações

[38] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 30 jun. 2023.

acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" e em seu parágrafo 2º determina que as medidas em questão deverão ser observadas "desde a fase de concepção do produto ou do serviço até a sua execução". Isso se complementa com o princípio da prevenção previsto no art. 6º, VIII, que exige a implementação de medidas para evitar a ocorrência de danos decorrentes do tratamento de dados pessoais.

Essas medidas organizacionais devem ser entendidas como quaisquer métodos ou meios que o responsável pelo tratamento de dados possa empregar para aplicar efetivamente os princípios de proteção de dados, garantindo os direitos e liberdades dos titulares dos dados (EDPB, 2020a, p.6). Além de ser uma ferramenta para garantir direitos e liberdades, o *PbD* também possibilita o estabelecimento de uma relação de confiança com o titular dos dados (Lemos; Branco, 2021, p.458).

À vista disso, durante a concepção de uma interface gráfica de um site ou aplicativo, é imprescindível que se desenvolva recursos e funcionalidades que estejam em conformidade com os princípios de proteção de dados. Isso implica, dentre outras coisas, em minimizar a coleta de dados pessoais, promover transparência e clareza na comunicação com os usuários, assegurar a segurança do tratamento desses dados e fornecer mecanismos para que os usuários possam exercer seus direitos e tomar decisões informadas. A esse respeito, a EDPB destaca alguns elementos chaves que devem ser considerados para a aplicação do *PbD:*

> - Autonomia: é fundamental garantir aos titulares dos dados o máximo grau possível de autonomia para determinar o uso de seus dados pessoais, bem como ter controle sobre o escopo e as condições desse uso ou tratamento;
> - Interação: os titulares dos dados devem ter a capacidade de se comunicar e exercer seus direitos em relação aos dados pessoais tratados pelo controlador.
> - Expectativa: o tratamento dos dados deve estar alinhado com as expectativas razoáveis dos titulares dos dados.
> - Escolha do consumidor: os controladores não devem restringir injustamente seus usuários, como, por exemplo, "prender" o titular em seu serviço, impedindo-o de exercer seu direito de portabilidade dos dados;
> - Equilíbrio de poder: alcançar um equilíbrio de poder é um objetivo fundamental na relação entre o controlador e o titular dos dados. Devem ser evitados desequilíbrios de poder e, quando isso não for possível, eles devem ser reconhecidos e contramedidas adequadas devem ser adotadas.
> - Não enganar: as informações e opções relacionadas ao tratamento de dados devem ser fornecidas de maneira objetiva e neutra, evitando qualquer linguagem ou design enganoso ou manipulador;
> - Veracidade/Honestidade: os controladores devem disponibilizar informações sobre como tratam os dados pessoais, agir de acordo com suas

> declarações e não enganar os titulares dos dados (EDPB, 2022, p.10, tradução nossa)

Nesse contexto, quando os agentes de tratamento utilizam técnicas manipulativas, como confundir ou forçar o titular a compartilhar mais dados do que desejado, eles afrontam o princípio do *privacy by design*. Enquanto os *dark patterns* buscam enganar e manipular os usuários em seu processo de tomada de decisão, o *PbD* visa estabelecer a confiança do usuário, colocando-o em posição central e fornecendo as ferramentas necessárias para que suas decisões sejam feitas de forma consciente.

Reconhecendo que a utilização de designs enganosos afronta diretamente o *PbD,* em fevereiro de 2023 a *Garante per la protezione dei dati personali (GPDP)*, autoridade de proteção de dados italiana, impôs à empresa Ediscom S.p.A multa de 300 mil euros por ter utilizado padrões obscuros, conduta que violava o art. 25, e outros, do GDPR[39].

Do boletim apresentado pela autoridade italiana, retira-se que durante a análise dos portais gerenciados pela empresa, foi observada a utilização de modelos de comunicação pouco claros, com ênfase no design gráfico das interfaces e nos métodos de registro de serviços. Além disso, em alguns dos portais examinados, durante o processo de registro, os usuários foram solicitados a fornecer consentimento específico para o processamento de dados para fins de marketing e comunicação com terceiros para fins de marketing. Caso uma das opções não fosse selecionada, um pop-up enfatizava a falta de consentimento e apresentava um botão de aceitação, mas o link para continuar sem aceitar era colocado em uma posição menos visível, o que poderia levar a uma emissão de consentimento não consciente ou por pressa para finalizar o processo.

Em sua decisão, a autoridade considerou que as práticas utilizadas levantavam dúvidas sobre a liberdade e consciência da vontade do usuário, concluindo que a coleta de consentimento não estava em conformidade com a legislação aplicável.

Na mesma direção, o EDPB, em seu guia orientativo sobre *data protection by design and by default,* cita que o a apresentação de opções de processamento de dados de maneira que dificulte para o titular se abster de compartilhar suas informações ou que crie obstáculos para o titular ajustar as configurações de privacidade para limitar o processamento são exemplos de *dark patterns* que, por sua vez, contrariam o espírito do art. 25 do GDPR, que, como demonstrado, dispõe sobre o *privacy by design.* O Comitê complementa pontuando que

---

[39] Disponível em: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9870014. Acesso em: 13. jul. 2023.

as opções predefinidas para o tratamento não devem ser invasivas e as opções de tratamento devem ser apresentadas de forma a não pressionar o titular dos dados a dar o seu consentimento (EDPB, 2020a, p.19).

4.4 O PAPEL DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Conforme evidenciado, devido às restrições inerentes ao titular, à disparidade de informações entre o titular e as organizações, bem como à intrincada natureza dos procedimentos de processamento de dados no ambiente digital, a mera ação individual para salvaguardar os próprios interesses não consegue assegurar uma proteção suficiente, fazendo-se necessário, portanto, a existência de um controle coletivo. Em vista disso, a intervenção da Autoridade Nacional de Proteção de Dados (ANPD) se torna fundamental para garantir o devido respeito e efetivação do direito fundamental à proteção dos dados pessoais dos cidadãos.

Conforme estabelecido no artigo 55-J da Lei Geral de Proteção de Dados (LGPD), é responsabilidade da ANPD, entre outras atribuições, garantir a salvaguarda dos dados pessoais, supervisionar e impor penalidades em casos de tratamento de dados em desconformidade com a regulamentação, conduzir pesquisas e desenvolver análises relacionadas às práticas de proteção de dados, e incentivar a adoção de padrões em serviços e produtos que facilitem o controle exercido pelos titulares sobre seus dados pessoais.

Desse modo, tendo em conta que a utilização de padrões obscuros nos tratamentos de dados pessoais infringe a LGPD, cabe à ANPD a fiscalização e o devido sancionamento das organizações que lançarem mão desse artifício. Nesse ponto, é oportuno destacar que, para promover a análise e fiscalização de padrões de design e interfaces, é necessário que a Autoridade tenha pessoal com capacidade técnica para tanto, o que implica em ter em seu quadro designers, psicólogos e especialistas em economia comportamental, por exemplo.

Outro ponto que merece atenção é que os profissionais de desenvolvimento e design utilizam códigos, terminologias específicas e diversas ferramentas, como guias, padrões de design e métodos como canvas. Essas práticas de design, ao serem amplamente adotadas, tendem a padronizar as interações e interfaces, resultando na criação de gramáticas de interfaces que fundamentam as interações entre humanos e produtos digitais (CNIL, 2019, p.42). Nesse cenário, convém que a ANPD promova debates e discussões acerca do tema com esses profissionais, possibilitando o compartilhamento de abordagens e práticas de

privacidade, fomentando, assim, a criação de métodos de design de privacidade e a formação de uma comunidade de design dedicada a esse assunto (CNIL, 2019, p.43).

É importante, ainda, que a ANPD também participe da construção dessa comunidade fornecendo guias de boas práticas de design. Um bom exemplo a ser tomado como referência é o trabalho desenvolvido pela CNIL, que possui uma página na internet (https://design.cnil.fr/en/) específica para tratar do assunto, onde disponibiliza recomendações, ferramentas abertas, estudos de casos, exemplos, etc, de padrões éticos de design com foco na proteção dos dados dos usuários titulares.

Por fim, é essencial que a ANPD atue de forma cooperativa com agências e autoridades de proteção ao consumidor no intuito de identificar padrões ilegais e implementar sanções adequadas (Marques; Mendes; Bergstein, 2023, p.8).

5 CONCLUSÃO

Traçada a linha argumentativa indicada na introdução desta dissertação, eis que é apropriado fornecer uma resposta ao problema de pesquisa apresentado nos seguintes termos: *à luz do regime de proteção de dados brasileiro, é legítima a utilização dos considerados dark patterns no design da interface de sites e aplicativos*? Não. A partir de uma análise detida acerca das principais características dos padrões obscuros, concluiu-se que sua utilização afronta princípios elementares do direito à proteção dos dados pessoais.

A fim de proporcionar uma estrutura mais coesa para as conclusões finais, apresenta-se a seguir as observações conclusivas elaboradas ao longo desta pesquisa:

1. O controle do indivíduo sobre suas informações ainda possui papel preponderante nas legislações modernas de proteção de dados pessoais, inclusive a LGPD, que tem como um de seus fundamentos a autodeterminação informativa (art.2º, II).
2. O controle individual tem como pressuposto que o titular de dados é um agente racional, capaz de analisar todas as nuances que envolvem o tratamento de seus dados. Contudo, o indivíduo não consegue acompanhar a complexidade do tratamento de dados e seus efeitos, especialmente no ambiente digital, e tende a ser influenciado por vieses cognitivos. Tem-se, portanto, que ao invés de *homo economicus,* o titular deve ser considerado como *homo manipulable.* De outra forma, a racionalidade do indivíduo é limitada, sendo o mesmo vulnerável diante do responsável pelo tratamento.

3. As decisões tomadas pelo titular de dados em sites e aplicativos são mediadas pela arquitetura de escolha, uma vez que somente as opções disponibilizadas podem ser selecionadas. Dessa forma, o design tem o potencial de restringir certas decisões individuais ao limitar seu âmbito de ação, bem como de incentivar a adoção de determinadas escolhas. Além disso, as pessoas reagem ao design de maneiras previsíveis, o que torna sua manipulação relativamente fácil.
4. Caracteriza-se como *dark pattern* o design com caráter manipulativo, que afeta diretamente o processo decisório do usuário; que seja capaz de causar prejuízo ao indivíduo; e que é aplicado com o intuito de beneficiar o fornecedor do produto/serviço. Os *dark patterns* utilizados no contexto de tratamento de dados incentivam o compartilhamento de dados para além do necessário ou influencia negativamente na tomada de decisão do titular em relação aos seus dados, interferindo na capacidade do titular proteger seus dados pessoais.
5. A aplicação de *dark patterns* nas atividades de tratamento de dados viola o princípio da boa-fé objetiva, conforme estabelecido pelo artigo 6º da LGPD. Isso se dá pelo fato de que a boa-fé requer que os responsáveis pelo tratamento dos dados ajam com integridade e honestidade, demonstrando transparência e colaboração com o titular, o que, por sua vez, contribui para mitigar o desequilíbrio de informações existente entre as partes. Em contrapartida, os padrões obscuros têm uma natureza manipuladora, cujo objetivo é dificultar a tomada de decisão consciente por parte do titular ou até mesmo levá-lo a escolhas que sejam contrárias aos seus interesses. Isso ocorre mediante a exploração das limitações do titular.
6. O consentimento obtido através de um design enganoso é considerado inválido, de acordo com o disposto no artigo 9º, §1º, da LGPD. Isso ocorre porque os *dark patterns,* dependendo do tipo empregado, têm a capacidade de distorcer os elementos que compõem a validade do consentimento. Além disso, foi observado que, embora mais comum em situações que se baseiam no consentimento para o tratamento de dados, os padrões obscuros também podem ser aplicados em contextos que envolvam diferentes fundamentos legais, como a execução de contratos e o legítimo interesse.
7. A aplicação de *dark patterns* afronta o princípio do *privacy by design.* Enquanto os *dark patterns* buscam enganar e manipular os usuários em seu processo de tomada de decisão, o *privacy by design* se concentra em construir a confiança do usuário, priorizando sua posição e disponibilizando as ferramentas essenciais para que suas escolhas sejam efetuadas de maneira informada e consciente.

8. Para além da sua função de supervisão e aplicação de sanções aos responsáveis pelo tratamento de dados que empreguem *dark patterns*, cabe à ANPD promover a discussão em torno do design voltado à privacidade, estabelecendo espaços de diálogo com especialistas do campo. Ademais, a autoridade deve disponibilizar diretrizes e direcionamentos relativos a padrões éticos de design, com ênfase na salvaguarda dos dados pessoais dos usuários titulares, e trabalhar em cooperação com agências e autoridades de proteção ao consumidor no intuito de identificar padrões ilegais.

REFERÊNCIAS

ACQUISTI, Alessandro; GROSSKLAGS, Jens. Privacy and Rationality in Individual Decision Making. **IEEE Security & Privacy**. January/February, p.24-30, 2005.

ACQUISTI, Alessandro; GROSSKLAGS, Jens. What can behavioral economics teach us about privacy? In ACQUISTI, Alessandro *et.al*. **Digital Privacy**: theory, Technologies and practices. Auerbach Publications, p.363-377, 2008.

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and human behaviour in the age of information. **Science**, v. 347, p. 509-514, 30 jan. 2015.

ACQUISTI, Alessandro et al. **Nudges for Privacy and Security**: Understanding and Assisting User's Choices Online. 50 ACM Computing Surveys, Vol 50, Nº 3, Article 44, 2007.

ACQUISTI, Alessandro; BRANDIMARTE, Laura; LOEWENSTEIN, George. Privacy and behavioral economics. In KNIJNENBURG, Bart P. *et.al*. **Modern Socio-Technical Persctives on Privacy**. Springer, 2022.

AGRE, Philip E. Introduction. In: AGRE, Philip E.; ROTENBERG, Marc (Orgs.). **Technology and Privacy:** The New Landscape. London-Cambridge: The MIT Press, 1997.

AMERICAN PSYCHOLOGICAL ASSOCIATION. **APA dictionary of psychology**. Disponível em: https://dictionary.apa.org/. Acesso em: 20 mar. 2023.

AVILA, F. e BIANCHI, A. (Orgs.) (2015). **Guia de Economia Comportamental e Experimental**. São Paulo. EconomiaComportamental.org. Disponível em: <www.economiacomportamental.org>.

BAILLO TARGA, M. L.; RIEMENSCHNEIDER, P. S. Função hermenêutica do princípio da boa-fé objetiva: interpretação dos contratos nas relações civis e de consumo. **civilistica.com**, v. 11, n. 3, p. 1-28, 25 dez. 2022.

BENJAMIN, Antonio Herman V.; MARQUES, Claudia Lima; BESSA, Leonardo Roscoe. **Manual de direito do consumidor** [livro eletrônico]. 9. ed. São Paulo: Thomson Reuters Brasil, 2021.

BENNETT, Colin J.; RAAB, Charles D. **The Governance of Privacy**: Policy Instruments in Global Perspective. 1. ed. London-New York: Routledge, 2003 (EPUB).

BIONI, Bruno Ricardo. **Proteção de dados pessoais***:* a função e os limites do consentimento. 3. Reimpr. Forense: Rio de Janeiro, 2019.

BORGESIUS, Zuiderveen Borgesius, F. J. **Improving privacy protection in the area of behavioural targeting**. 2014. PhD thesis. Faculty of Law, University of Amsterdam, 2014.

BÖSCH, Christoph *et al*. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *In:* **Proceedings on Privacy Enhancing Technologies**. v.4, p.237-254, 2016.

BRASIL. **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm.

BRASIL. **Lei n. 12.414, de 9 de junho de 2011**. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm

BRASIL. **Lei n. 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

BRIGNULL, Harry. **Dark Patterns**: Deception vs. Honesty in UI Design (November 1, 2011). Disponível em: <https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design>. Acesso em: 24 fev. 2023.

BRIGNULL, Harry. **Deceptive patterns***:* exposing the tricks tech companies use to control you. Testimonium Ltda. Digital edition. 2023. E-book.

CALO, Ryan. Privacy, Vulnerability, and Affordance. **DePaul Law Review**, v. 66, 2017.

CAVOUKIAN, Ann. **Privacy by design***:* the 7 foundational principles. 2011. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 11 jul. 2023.

COMISSION NATIONALE I'INFORMATIQUE ET DES LIBERTÉS (CNIL). **Shaping choices in the digital world** – from dark patterns to data protection: the influence of ux/ui design on user empowerment. IP Reports: Innovation and Foresight. nº 06, 2019. Disponível em: https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Privacidade e proteção de dados pessoais 2021** [livro eletrônico]: perspectivas de indivíduos, empresas e organizações públicas no Brasil, São Paulo, 2022. Disponível em:

https://cetic.br/media/docs/publicacoes/2/20220817110001/privacidade_protecao_de_dados_pessoais_2021_livro_eletronico.pdf.

COMPETITION & MARKETS AUTHORITY (CMA). **Online choice architecture**. How digital design can harm competition and consumers. 2022. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1066524/Online_choice_architecture_discussion_paper.pdf. Acesso em: 07 abr. 2023.

COMPETITION & MARKETS AUTHORITY (CMA) **Online platforms and digital advertising** - Market study. Appendix Y: choice architecture and Fairness by Design. 2020. Disponível em: https://assets.publishing.service.gov.uk/media/5fe36ab9d3bf7f0898e0776c/Appendix_Y_-_choice_architecture_and_Fairness_by_Design_1.7.20.pdf.

CONTI, Gregory; SOBIESK, Gregory. Malicious Interface Design: Exploiting the User. *In:* **Proceedings of the 19th International Conference on World wide web**, 2010, Raleigh. New York: Association for Computing Machinery, 2010, p.271-280.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In*: DONEDA, Danilo et al (coords). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

ESTADOS UNIDOS DA AMÉRICA. **California Consumer Privacy Act**, California Civil Code §§ 1798.100-1798.199(2020). Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 10 jul. 2023.

ESTADOS UNIDOS DA AMÉRICA. **California Privacy Rights Act,** California Civil Code §§ 1798.100-1798.199(2020). Disponível em: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Acesso em: 10 fev 2023.

ESTADOS UNIDOS DA AMÉRICA. Text - S.3330 - 117th Congress (2021-2022): **DETOUR Act**. Congress.gov, Library of Congress, 07/12/2021. Disponível em: https://www.congress.gov/bill/117th-congress/senate-bill/3330/text. Acesso em: 13 mar. 2023.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 4/2019 on Article 25 Data protection by design ad by default**. Version 2.0. 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 05/2020 on consent under Regulation 2016/679**. Version 1.0. 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 3/2022 on Dark patterns in social media platform interfaces***:* how to recognise and avoid them. Version 1.0. 2022. Disponível em: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf.

FEDERAL TRADE COMISSION. **Bringing dark patterns to light**, 2022. Disponível em: https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.

FORBRUKERRADET. **You can log out, but you can never leave***:* How Amazon manipulares consumers to keep them subscribed to Amazon Prime. 2021. Disponível em: https://storage02.forbrukerradet.no/media/2021/01/2021-01-14-you-can-log-out-but-you-can-never-leave-final.pdf.

FORBRUKERRADET. **Deceived by design***:* How tech companies use dark patterns to discourage us form exercising our rights to privacy. 2018. Disponível em: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

FUTURE OF PRIVACY FORUM. **Unlocking data protection by design & by default***:* lessons from the enforcement of article 25 GDPR. 2023. Disponível em: https://fpf.org/wp-content/uploads/2023/05/FPF-Article-25-GDPR-A4-FINAL-Digital.pdf.

GIGERENZER, Gerd; GAISSMAIER, Wolfgang. Heuristic Decision Making. **Annual Review of Psychology**, v. 62, p.451-482, 2011.

GUSTIN, Miracy Barbosa de Souza; DIAS, Maria Tereza Fonseca. **(Re)pensando a pesquisa jurídica***:* teoria e prática. 3.ed. rev. atual. Belo Horizonte: Editora Del Rey, 2010.

HARTZOG, Woodrow. Opinions – The Case Against Idealising Control. **European Data Protection Law Review**, v. 4, n. 4, p. 423–432, 2018a.

HARTZOG, Woodrow. **Privacy's blueprint***:* the battle to control the design of new technologies. Cambridge, Massachusetts: Harvard University Press, 2018b.

HOEPMAN, Jaap-Henk. Privacy Design Strategies. In: CUPPENS-BOULAHIA, N. et al (eds). ICT Systems Security and Privacy Protection. SEC 2014. **IFIP Advances in Information and Communication Technology**. Springer, Berlin, Heidelberg, v. 428, 2014.

HOOFNAGLE, Chris Jay; URBAN, Jennifer M. Alan Westin's Privacy Homo Economicus, **Wake Forest Law Review**, v.49, p.261-317, 2014.

JAROVSKY, Luiza. **Dark patterns in personal data collection***:* definition, taxonomy and lawfulness. 1 mar. 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4048582.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA). **Study on Monetising Privacy**: An Economic Model for Pricing Personal Information. European Union Agency for Network and Inf. Sec. (ENISA), 2012. Disponível em: https://www.enisa.europa.eu/publications/monetising-privacy.

JOHNSON, Eric J. **The elements of choice***:* why the way we decide matters. New York: Riverhead Books, 2021.

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

KONSUMENTVERKET. **Underlagsrapport 2021:1**. Barriers to a well-functiong digital market – effects of visual design and information disclosures on consumer detriment. Disponível em: < https://www.medvetenkonsumtion.se/wp-content/uploads/2021/05/Konsumentverket-underlagsrapport-barriers-digital-market.pdf>. Acesso em: 14 abr. 2023.

KYI, Lin *et al.* Investigating Deceptive Design in GDPR's Legitimate Interest. *In*: **Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (CHI'23)**, 2023, Hamburg. New York: Association for Computing Machinery, 2023, p. 1-16.

LAZARO, Chistophe; MÉTAYER, Daniel Le. Control over Personal Data: True Remedy or Fairy Tale? **SCRIPT-ed**, v. 12, n. 1, p. 3-34, 2015.

LEMES, David de Oliveira. Aspectos gerais de uso das interfaces gráficas de usuários. **Revista Digital de Tecnologias Cognitivas**, n. 18, jul./dez. 2018.

LEMOS, Ronaldo; BRANCO, Sérgio. Privacy by design*:* conceito, fundamentos e aplicabilidade na LGPD. *In:* DONEDA, Danilo et al (coords). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

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

MACHADO, Diego Carvalho. **A regulação das tecnologias de perfilamento no direito brasileiro***:* articulando direito e tecnologia para a promoção da proteção de dados desde a concepção. 2022. Tese de Doutorado em Direito – Faculdade de Direito, Universidade do Estado do Rio de Janeiro, Rio de Janeiro, 2022.

MALGIERI, Gianclaudio; NIKLAS, Jedrzej. Vulnerable data subjects. **Computer Law & Security Review,** v. 37, 2020.

MALGIERI, Gianclaudio. The concept of fairness in the GDPR. A linguisti and contextual interpretation. *In:* **Proceedings of the 2020 Conference on Fairness, Accountability and Tranparency**. New York: Association for Computing Machinery, 2020, p.154-166.

MARTINS-COSTA, Judith. **A boa-fé no direito privado***:* critérios para a sua aplicação. 2ª ed. São Paulo: Saraiva, 2018. E-book.

MATHUR, A.; KSHIRSAGAR, M.; MAYER, J. What Makes a Dark Pattern... Dark?: Design Attributes, Normative Considerations, and Measurement Methods. *In:* **Proceedings of the 21 CHI Conference on Human Factors in Computing Systems**, 2021, Yokohama. New York: Association for Computing Machinery, 2021, p.1-18.

MATHUR, Arunesh *et al*. Dark patterns at scale: Findings from a crawl of 11K shopping websites. *In:* **Proceedings of the ACM on Human-Computer Interaction**, v. 3, n. CSCW, 2019, p.1-32.

MARQUES, Cláudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. Dark patterns e padrões comerciais escusos. **Revista de Direito do Consumidor**. vol. 145/2023, p. 295 – 316. Jan – Fev, 2023.

MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. In: AGRE, Philip; ROTENBERG, Marc. (orgs.). **Technology and privacy**: The new landscape. Cambridge: MIT Press, 1997.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014. E-book.

MENDES, Laura Shertel; RODRIGUES JÚNIOR, Otávio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a proteção constitucional dos dados pessoais*:* rumo a um direito fundamental autônomo. *In:* DONEDA, Danilo et al (coords). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MILLER, Arthur. **The Assault on Privacy**. Ann Arbor: University of Michigan Press, 1971.

MIRAGEM, Bruno. **Curso de direito do consumidor**. 6.ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2016.

MIRAGEM, Bruno. Princípio da vulnerabilidade: perspectiva atual e funções no direito do consumidor contemporâneo. In: MIRAGEM, Bruno; MARQUES, Claudia Lima; MAGALHÃES, Lucia Ancona Lopez de. (Org.). **Direito do Consumidor**: 30 anos do CDC. 1ª. Ed. São Paulo: Forense, 2020.

NEGRI, Sérgio Marcos Carvalho de Ávila; MACHADO, Joana de Souza; GIOVANINI, Carolina Fiorini Ramos. Nem invisíveis, nem visados*:* inovação, direitos humanos e vulnerabilidade de grupos no contexto da Covid-19. In: **Liinc em Revista**, Rio de Janeiro, v.16, n.2, e5367, dezembro 2020.

NISSEMBAUM, Hellen. **Privacy in context***:* technology, policy, and the integrity of social life. Stanford Law Books, 2009.

NISSENBAUM, Helen. Contextual approach to privacy online. **Daedalus**, v.140**,** p.32-48, 2011.

NORMAN, Don. **The design of everyday things**. Revised and expanded edition. Basic Books: 2013.

NORMAN, Don. **The Four Fundamental Principles of Human-Centered Design and Application**. 2019. Disponível em: https://jnd.org/the-four-fundamental-principles-ofhuman-centered-design/. Acesso em: 04 ago. 2023.

ORGANIZATION OF ECONOMIC CO-OPERATION AND DEVELOPMENT. **Dark commercial patterns**. 2022. Disponível em: https://www.oecd-ilibrary.org/docserver/44f5e846-en.pdf?expires=1692890382&id=id&accname=guest&checksum=BDA276928DD452FE718E796E46D3F9D1.

PEREIRA, Caio Mário da Silva. **Instituições de direito civil***:* Volume III. Contratos. 1ª ed. Eletrônica. Rio de Janeiro: 2013.

RODOTÀ, Stefano. **A vida na sociedade da vigilância***:* a privacidade hoje. Org. Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SOLOVE, Daniel. **Understanding privacy**. Cambridge: Harvard University Press*,* 2008.

SOLOVE, Daniel J. Introduction: Privacy Self-Management and the Consent Dilemma. **Harvard Law Review**, v. 126, n. 7, p. 1880–1903, 2013.

SCHWARTZ, Paul. Privacy and democracy in cyberspace. **Vanderbilt Law Review**, v.52, p.1609-1701, 1999.

SCHWARTZ, Paul. Internet privacy and the state. **Connecticut Law Review**, v. 32, p.815-859, 2000.

SARLET, Ingo Wolfgang. O direito fundamental à proteção de dados. *In:* DONEDA, Danilo et al (coords). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

TEPEDINO, Gustavo; SCHREIBER, Anderson. Os efeitos da constituição em relação à cláusula de boa-fé no código de defesa do consumidor e no código civil. **Revista da EMERJ**, v. 6, n. 23, p.139-151, 2003.

UNIÃO EUROPEIA. Carta dos direitos fundamentais da União Europeia (2016/C 202/02). **Jornal Oficial da União Europeia**, 07/06/2016. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR>. Acesso em: 10 fev. 2023.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Estrasburgo, 04/05/2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32022R2065. Acesso em: 11 mai. 2023.

UNIÃO EUROPEIA. Regulamento (UE) nº 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022 relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais). **Jornal Oficial da União Europeia**, Estrasburgo, 27/10/2022. Disponível em: https://eur-lex.europa.eu/legalcontent/ PT/TXT/PDF/?uri=CELEX:32016R0679&from=DA. Acesso em: 11 mai. 2023.

TVERSKY, Amos; KAHNEMAN, Daniel. Judgment under uncertainty: heuristics and biases. **Science, New, Series**, v. 85, 1974, p.1124-1131.

THALER, Richard H.; SUNSTEINS, Cass R. **Nudge:** como tomar melhores decisões sobre saúde, dinheiro e felicidade. 1.ed. Rio de Janeiro: Objetiva, 2019.

URBAN, Jennifer M; HOOFNAGLE, Chris Jay. The Privacy Pragmatic as Privacy Vulnerable. *In:* **Symposium on Usable Privacy and Security (SOUPS 2014) Workshop on Privacy Personas and Segmentation (PPS)**, 2014, Menlo Park. UC Berkeley Public Law, 2014.

WALDMAN, Ari E. Privacy, Notice, and Design. **Stanford Technology Law Review**, v.21, p.74-127, 2018.

WALDMAN, Ari Ezra. Cognitive Biases, Dark Patterns, and the 'Privacy Paradox. **Current Issues in Psychology**, v.31, p.105-109, 2020.

WARREN, Samuel; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. 4, n. 5, 1890.

WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967.