INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA
ESCOLA DE DIREITO E ADMINISTRAÇÃO PÚBLICA
MESTRADO PROFISSIONAL EM DIREITO

PADRÕES OBSCUROS E CONSENTIMENTO DO TITULAR DE DADOS PESSOAIS NO ÂMBITO DO COMÉRCIO ELETRÔNICO

Carlos Eduardo Marques Silva
Orientadora: Profª. Drª. Laura Schertel Mendes
Coorientador: Prof. Dr. Guilherme Pereira Pinheiro

Brasília-DF
2024

CARLOS EDUARDO MARQUES SILVA

PADRÕES OBSCUROS E CONSENTIMENTO DO TITULAR DE DADOS PESSOAIS NO ÂMBITO DO COMÉRCIO ELETRÔNICO

Dissertação apresentada ao programa de pós-graduação em Direito, como parte do requisito para a obtenção do título de Mestre no Mestrado Profissional em Direito do Instituto Brasileiro de Ensino e Pesquisa – IDP.

Orientadora: Profa. Dra. Laura Schertel Mendes
Coorientador: Prof. Dr. Guilherme Pereira Pinheiro

Código de catalogação na publicação – CIP

S586p Silva, Carlos Eduardo Marques

Padrões obscuros e consentimento do titular de dados pessoais no âmbito do comércio eletrônico / Carlos Eduardo Marques Silva. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2024.

131 f. : il.

Orientadora: Profª. Drª. Laura Schertel Mendes.
Coorientador: Prof. Dr. Guilherme Pereira Pinheiro.

Dissertação (Mestrado Profissional em Direito) — Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2025.

1. Proteção de dados pessoais. 2. Consentimento 3 Comércio eletrônico. I.Título

CDDir 341.2738

Elaborada por Pollyana da Silva Marra – CRB 1/3704

INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA

PROGRAMA DE PÓS GRADUAÇÃO STRICTO SENSU EM DIREITO

MESTRADO PROFISSIONAL EM DIREITO ECONÔMICO E DESENVOLVIMENTO

Ata de Defesa de Dissertação

Discente: Carlos Eduardo Marques Silva
Registro Acadêmico: 2224031
Orientador(a): Profa. Dra. Laura Schertel Mendes
Coorientador(a) (se houver): Prof. Dr. Guilherme Pereira Pinheiro

Título do trabalho apresentado:

PADRÕES OBSCUROS E CONSENTIMENTO DO TITULAR DE DADOS PESSOAIS NO ÂMBITO DO COMÉRCIO ELETRÔNICO

Resultado:

Após o exame do trabalho e da apresentação oral do Projeto de Dissertação e arguição do(a) candidato(a) a banca examinadora decidiu pela: Aprovação

Observações:

Sem observações.

Assinatura da banca examinadora

Profa. Dra. Laura Schertel Mendes	Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP
Profa. Dra. Taina Aguiar Junquilho	Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP
Prof. Dr. Luís Felipe Perdigão de Castro	"Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa - IDP"
Prof. Dr. Diógenes Faria de Carvalho	Faculdade Autônoma de Direito - FADISP

O presente documento possui caráter comprobatório para fins de registro de participação docente na respectiva banca avaliadora.
Para mais informações, contate ppgdireito@idp.edu.br

4/12/2024 2:30pm

SGAS Quadra 607 - Módulo 49
Via L2 Sul, Brasília - DF
CEP 70.200-670

(61) 3535-6565

CARLOS EDUARDO MARQUES SILVA

PADRÕES OBSCUROS E CONSENTIMENTO DO TITULAR DE DADOS PESSOAIS NO ÂMBITO DO COMÉRCIO ELETRÔNICO

Dissertação apresentada ao programa de pós-graduação em Direito, como parte do requisito para a obtenção do título de Mestre no Mestrado Profissional em Direito do Instituto Brasileiro de Ensino e Pesquisa – IDP.

Aprovado em 04/02/2025

Banca Examinadora

Profa. Dra. Laura Schertel Mendes
Orientadora - IDP

Prof. Dr. Guilherme Pereira Pinheiro
Coorientador - IDP

Profa. Dra. Tainá Aguiar Junquilho
Convidada - IDP

Prof. Dr. Luís Felipe Perdigão de Castro
Convidado - IDP

Prof. Dr. Diógenes Faria de Carvalho
Convidado - USP

AGRADECIMENTOS

O Mestrado Profissional do IDP tornou-se um objetivo meu quando eu ainda estava na graduação. Iniciei a pesquisa sobre proteção de dados pessoais ao final do curso, quando estava produzindo a minha monografia e tive acesso ao livro "Privacidade, proteção de dados pessoais e defesa do consumidor: linhas gerais de um novo direito fundamental" da professora Doutora Laura Schertel Mendes. Quando me deparei com a obra em 2019 o assunto para mim era apenas superficial, muitas pessoas comentavam, mas não havia nenhum nível de profundidade. No entanto, após a leitura dessa obra, os horizontes se expandiram para mim, além de ser um campo muito recente no direito, a proteção de dados pessoais me trouxe perspectivas de trabalho, estudo e de futuro.

Dali em diante eu sabia que tinha um objeto de pesquisa orientado para o futuro, queria me debruçar sobre a proteção de dados pessoais e me tornar um dos juristas que forma autoridade no tema. Foi isso que me motivou buscar o Mestrado Profissional em Direito do IDP, pois eu já trabalhava, à época do ingresso, com o tema no âmbito do Setor de Telecomunicações, quando estávamos construindo o Manual de boas práticas em proteção de dados do setor, que inclusive foi elaborado sob a orientação da Dra. Laura Schertel Mendes.

A oportunidade de pesquisar sobre esse tema tendo a orientação da Professora Dra. Laura me deixa profundamente agradecido, sem dúvidas isso marcará toda a minha trajetória profissional e acadêmica. Grande gratidão tenho também ao meu coorientador, o Professor Dr. Guilherme Pereira Pinheiro, com quem tive a oportunidade de aprender muito sobre assuntos relacionados à tecnologia e privacidade na disciplina do Mestrado "Direito, Internet e Sociedade", e que tive uma rica troca, sobretudo pelos seus conhecimentos vastos em naturalidade de rede e a formação internacional que lhe permitiu trazer para a sala de aula um resumo do que e como acontece no mundo.

Sou muito feliz por ter recebido uma rica orientação por parte do Professor Dr. Luís Felipe Perdigão de Castro, que foi o meu professor na disciplina de Metodologia da Pesquisa em Direito. Os seus ensinamentos me orientaram para uma escrita propositiva e com profundidade, sempre fugindo de entregar "mais do mesmo". Ele me ajudou a atribuir personalidade ao meu texto, me mostrando que a forma como nos comunicamos refletem inclusive a nossa história.

Agradeço também à Professora Dra. Tainá Junquilho, um grande expoente da Inteligência Artificial, que me ensinou muito na disciplina que cursei sobre Regulação da Inteligência Artificial, e com quem tive trocas muito ricas, inclusive na minha banca de

qualificação, haja vista que as suas recomendações me trouxeram uma nova perspectiva sobre a minha pesquisa, me ajudando nesse processo de conclusão.

No IDP fiz irmãos que levarei por toda a vida, menciono aqui os meus queridos amigos Cinthia Portela, Sysley Sampaio, Luís Gustavo, Lorena Gargaglione, Rodrigo Alves, Marcos Antônio, Gabriela Miranda, Laysa Stone, Lilian Scavuzzi, Adrise Lagos, Ana Clara, Cyntya Melo, Anna Guimarães, Paula Vilela e Guilherme Theo Sampaio. Cada pessoa ao seu modo deixou a sua marca em minha vida, aprendi muito com todas elas, me senti e me sinto uma pessoa especial cada vez que converso com qualquer um desses amigos, e tenho visto o resultado de grandes parcerias que estamos construindo juntos.

O Mestrado para o Carlos Eduardo de 10 anos atrás não era verdadeiramente uma aspiração. Filho de camponeses e feirantes, fui criado em um ambiente que a academia científica não abrangia, afinal de contas, necessidades básicas eram sinônimo de conforto nesse tempo. Lembro de cada vez que eu não pude ir à escola com o transporte rural, porque havia atolado, ou caído alguma ponte, e eu voltava para casa desesperado para que o meu pai largasse o serviço, que na época era tirar leite, para me levar de moto a tempo da segunda aula. O coordenador da Escola à época, estimado prof. Rosivelton Amaral, já sabia quando isso acontecia e com um sorriso de canto de boca dizia, “essa chuva, né?”.

É fato que a realidade na Escola Pública é um tanto diferente da rede privada, ao invés de discussões sobre qual Universidade estudar, qual curso fazer, era corriqueiro escutar o que faríamos após o término do Ensino Médio? Eu tinha um sonho grande de cursar a faculdade de Direito, afinal de contas seria o primeiro da família a conseguir esse feito, em um curso considerado “de elite”. Sabendo das minhas limitações financeiras, tinha certeza de que precisava ser aprovado na Universidade Pública, que dentro do meu contexto era a Universidade Federal de Goiás. Ao comentar sobre isso com um professor que eu sabia que tinha estudado na mesma Universidade, ele me orientou a tentar fazer um curso menos concorrido, afinal de contas, Direito, Engenharia e Medicina eram cursos de elite e muito disputados.

Em um primeiro momento até acreditei que era um bom conselho, afinal de contas o Enem já estava chegando, e mesmo eu tendo me preparado muito, o curso de Direito ofertava apenas 6 vagas para alunos oriundos de escolas públicas e que aferir renda mínima per capita de até 1,5 salários-mínimos por pessoa no lar. Mas nessa caminhada conheci amigos extraordinários, que partilhavam do mesmo sonho que eu, que era cursar uma boa faculdade e mudar a história das nossas famílias. Juntos, estudamos e traçamos estratégias para enfrentar

o Enem, e todos nós tivemos grande sucesso. Fui aprovado no Curso de Direito da Universidade Federal de Goiás, onde a minha jornada jurídica começou.

No meu primeiro dia de aula eu fiz uma promessa a mim mesmo, de que eu honraria aquela cadeira que eu estava ocupando, por já saber àquela altura que o pagamento dos meus estudos estava recaindo justamente sobre aqueles que como os meus pais, mais sofrem com uma alta carga de tributos, pois as pequenas contribuições já significava muito, e é exatamente o que, somado, custeava a formação de tantas pessoas pelo Brasil afora. Eu não entrei na Universidade querendo mudar o mundo de todos, mas queria mudar a realidade da minha família, que era o meu mundo.

Muitas vezes eu me questionava se realmente teria sucesso em um curso cujos meus colegas, em sua maioria, pertencentes a famílias muito tradicionais, renomadas do ramo jurídico, estariam "disputando o mercado". Me recordo de diversos episódios em que eu estava na feira ajudando minha mãe, na nossa banca de queijos, eu pensava, será mesmo que eu conseguirei me consolidar como um jurista? Naquele contexto eu conseguia ver uma grande discrepância de realidades, mas que a cada reflexão, só me instigava a querer me superar em meus desafios.

Graças às grandes oportunidades que a UFG me deu, consegui desenvolver projetos incríveis na Iniciação Científica, tendo sido voluntário por dois anos (PIVIC) e bolsista (PIBIC) um ano, fui coordenador do Centro de Atendimento ao Consumidor Superendividado, projeto encabeçado pelo meu orientador o Prof. Dr. Diógenes Faria Carvalho, que foi e ainda é o meu mentor em minha trajetória acadêmica e profissional, e um dos grandes amigos que a UFG me trouxe. Ao concluir a Universidade já estava com algumas boas propostas de trabalho, tendo optado por ser Trainee Jurídico na Conexis Brasil Digital e dali em diante me vi imerso nesse universo da regulação, me aprofundando cada vez mais. Foi ali que tive contato com grandes expoentes da Regulação do Setor de Telecomunicações, e dentre eles a Dra. Daphne Nunes, que foi a minha mentora nesse âmbito e uma das pessoas que mais me encorajou a cursar o Mestrado em Direito do IDP. Tive a oportunidade de aprender muito também com o hoje grande amigo Bruno Cavalcanti, que mesmo em curto período, me contagiou com o seu senso de grandeza, me estimulando com palavras e atitudes incentivadoras.

Não sei se graças ao Destino, ou ao cumprimento de minha programação, no IDP tive a sorte de conhecer pessoas incríveis, dentre elas a Paula Vilela, em uma disciplina de Regulação sob a condução do Prof. Dr. Gustavo Justino. Na disciplina fizemos um trabalho em grupo, que foi um sucesso, eu e Paula ficamos muito felizes com o alinhamento de nossos

projetos, e de imediato já lhe dei a deixa, de que caso soubesse de alguma oportunidade de trabalhar com regulação em Brasília, estaria à disposição. Não demorou para ela me recomendar para o Diretor da ANTT, Guilherme Theo Sampaio, que hoje além de marido de Paula, é o meu chefe e grande amigo, em quem me inspiro por vê-lo como o meu grande referencial e mentor.

Após fazer um breve retrospecto da minha trajetória até chegar aqui, ocultando boa parte dos desafios e das conquistas, por falta de espaço nesse campo de agradecimentos, me vejo orgulhoso de estar finalizando o Mestrado Profissional em Direito em uma das maiores Escolas do país, e de maior renome.

Aproveito para agradecer ao meu noivo, Brenno Henrique, a quem amo muito, pela paciência e incentivo nesses anos de pesquisa. Sem o seu apoio e conselhos, essa caminhada seria bem mais desafiadora. Aos meus pais, Lessandra Marques e Valtoir Silva, por tudo o que fizeram e fazem por mim, e à minha irmã Maria Eduarda Marques, por ser o meu esteio e porto seguro. Às minhas avós, Luzimar Marques e Florecina Felipe, que muito me abençoam, e à memória de meu avô Libertino Domingues, que sempre me chamou de “meu doutor”.

Gratidão.

RESUMO

A proteção de dados pessoais tem ocupado o espaço de debate público nos últimos anos devido ao conhecimento popular a respeito das práticas de manipulação e modulação de comportamentos que podem ser realizadas a partir do tratamento dos dados. Não por outra razão, na economia moderna, os dados pessoais estão sendo considerados um grande ativo, comparado ao petróleo, em termos de rentabilidade. Os estatutos protetivos foram se desenvolvendo mundo afora na busca por regulamentar e regular a forma como se tem acesso aos dados pessoais dos indivíduos, tendo o seu ápice no GDPR na Europa que inclusive influenciou a construção da LGPD no Brasil. No entanto, apesar das disposições normativas importantes, sobretudo com a consagração da proteção de dados pessoais como um direito fundamental em 2022 pela Emenda Constitucional nº 115/2022, há ainda algumas dificuldades do ponto de vista regulatório em torno da matéria, haja vista a sua extensão e a constante evolução das mais diversas tecnologias da informação. Nesse contexto, a utilização de *dark patterns* surgem como um ponto de atenção no contexto da economia e do consumo influenciado e impulsionado por dados pessoais, ao passo que a sua utilização em interfaces na busca por obter do titular de dados o consentimento pode acabar por prejudicar a sua realização de forma válida, além de induzi-lo a erro. Desse modo, considerando as normativas de proteção de dados pessoais existentes no Brasil, sobretudo a LGPD, e as influências que ela recebe do GDPR e da tradição europeia de proteção de dados, a pesquisa buscará compreender como o uso de *dark patterns* pode comprometer a validade do consentimento obtido do titular no âmbito das relações de consumo, e consequentemente afetar o seu direito à proteção de dados pessoais e o que pode ser feito para contornar essa situação. A hipótese testada é de que a utilização dos *dark patterns* pode prejudicar a obtenção do consentimento do titular para a coleta e processamento de seus dados pessoais e ainda lhe causar prejuízos quando analisada sob o prisma das relações de consumo, incitando-o ao consumo inconsciente. O estudo foi organizado em três capítulos. No primeiro, propõe-se uma abordagem abrangente sobre a proteção de dados pessoais, passando desde o seu histórico, as gerações de direitos, até a sua positivação enquanto um novo direito fundamental no art. 5º da Constituição Federal de 1988. No segundo capítulo, realizou-se uma análise quanto ao consentimento do titular de dados pessoais, desde as bases conceituais, até a sua obtenção no âmbito do comércio eletrônico no cerne das relações de consumo. Ao final, em sede do terceiro capítulo, foi feito um estudo quanto às diretrizes nº 3/2022 da UE, sobre os *dark patterns*, e buscou-se tecer considerações a respeito de estratégias de contorno a esse fenômeno na atual conjuntura jurídica e regulatória brasileira.

Palavras-chaves: Padrões obscuros; Consentimento; Autodeterminação Informativa; Proteção de dados pessoais; Direito do Consumidor.

ABSTRACT

The protection of personal data has become a key topic of public debate in recent years, largely due to the growing awareness of how data can be manipulated and behavior shaped through it treatment. For this reason, personal data is increasingly being seen as a valuable asset in the modern economy, often compared to oil in terms of profitability. Protective statutes have been evolving worldwide in an effort to regulate access to individuals' personal data, with the General Data Protection Regulation (GDPR) in Europe being a landmark, which also influenced Brazil's General Data Protection Law (LGPD). However, despite these important legal frameworks, especially with the recognition of personal data protection as a fundamental right in Brazil with the Constitutional Amendment No. 115/2022, there remain several regulatory challenges, mainly due to the vast scope of data-related issues and the rapid advancement of information technologies. In this context, the use of dark patterns has emerged as a critical concern in the data-driven economy and consumer environment. These deceptive design techniques in user interfaces may lead data subjects to unknowingly give consent, potentially invalidating the process meas leading. Thus, this research seeks to explore how dark patterns, under Brazil's existing data protection laws, particularly the LGPD and the GDPR's influence, may undermine the validity of consent in consumer transactions and what steps can be taken to address this. The working hypothesis is that dark patterns can indeed compromise the consent process for data collection and processing, causing harm to consumers by leading them to unconscious consumption decisions. The study is structured in three chapters. The first chapter offers a comprehensive overview of personal data protection, tracing its historical development, the evolution of rights, and its recent recognition as a fundamental right under Article 5 of the 1988 Federal Constitution. The second chapter focuses on the concept of consent in personal data, examining its foundations and how it is obtained within the context of e-commerce and consumer relations. Finally, the third chapter addresses the European Union’s Guidelines No. 3/2022 on dark patterns and provides reflections on strategies to mitigate this issue in the current Brazilian legal and regulatory framework.

Keywords: Dark patterns. Consent. Informational self-determination. Personal data protection. Consumer rights.

LISTA DE TABELAS

SUMÁRIO

INTRODUÇÃO

A discussão a respeito da proteção à privacidade e aos dados pessoais tomou a pauta das diversas agendas políticas mundiais, sobretudo a partir do *boom* tecnológico verificado nos últimos 30 anos, com a evolução das tecnologias, da internet, criação das redes sociais e pela introdução da inteligência artificial na vida das pessoas. A preocupação quanto à segurança da informação, proteção à privacidade e proteção de dados pessoais, aumentou gradualmente, na medida em que diversos aplicativos, redes sociais, plataformas de compras on-line e outros instrumentos, para funcionarem de maneira assertiva, necessitam ser alimentados com os dados dos indivíduos que os utilizam.

Ainda que a evolução tecnológica tenha consolidado um cenário de diversas facilidades às pessoas, quando da inserção dos processos automatizados de coleta de dados, observou-se um agravamento da vulnerabilidade dos usuários. No entanto, como forma de mitigar tais situações, os países começaram a pensar formas de contornar a situação, criando uma série de protocolos e legislações, a exemplo da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, que disciplina o processo de coleta e processamento de dados pessoais, tendo como premissa o direito à informação e a obtenção do consentimento válido do usuário para a realização de tais processos.

Entretanto, o consentimento, para ser válido, deve ser "livre, informado, inequívoco e dizer respeito a uma finalidade determinada de forma geral e, em alguns casos, deve ser, ainda, específico"[1]. Isto é, a obtenção do consentimento de forma genérica e a partir da utilização de artifícios que dificultam a compreensão do usuário quanto aos termos da coleta, não pode revestir-se de validade.

Nesse sentido, mesmo com a previsão legal a respeito da necessidade de consentimento do titular de dados, há situações que aparentam relativizar a obtenção do consentimento obtido, como ocorre com o uso dos padrões obscuros, que podem ser listadas como falhas ou dificuldades dos sistemas automatizados, que induzem o usuário a anuir com a coleta e processamento de dados, sem, contudo, estar consciente de sua escolha.

---

[1]BIONI, Bruno. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. In: Minha Biblioteca, (3rd edição). Grupo GEN, 2021, p. 127.

Desse modo, considerando as normativas de proteção de dados pessoais existentes no Brasil, sobretudo a LGPD, e as influências que ela recebe do GDPR e da tradição europeia de proteção de dados, a pesquisa buscará compreender **como** o uso de *dark patterns* pode comprometer a validade do consentimento obtido do titular no âmbito das relações de consumo, e consequentemente afetar o seu direito à proteção de dados pessoais, e **o que** pode ser feito para contornar essa situação.

A hipótese testada é de que a utilização dos *dark patterns* pode prejudicar a obtenção do consentimento do titular para a coleta e processamento de seus dados pessoais e ainda lhe causar prejuízos quando analisada sob o prisma das relações de consumo, incitando-o ao consumo inconsciente.

A metodologia adota o método dialético dedutivo, estruturado em três principais etapas. Primeiramente, será realizada uma pesquisa bibliográfica abrangente, focando na literatura jurídica especializada nos temas abordados do estudo e na legislação europeia e brasileira sobre proteção de dados pessoais. Em seguida, será conduzido um estudo comparativo entre ambas as legislações, identificando convergências e divergências. A análise detalhada das Diretrizes nº 03/2022 do Comitê Europeu de Proteção de Dados (EDPB) servirá como um referencial crucial para entender os protocolos necessários para a utilização dos *dark patterns* sem prejudicar a obtenção do consentimento do titular de dados pessoais. Esta abordagem permitirá uma compreensão aprofundada das influências e adaptações necessárias para o contexto brasileiro, fundamentando as conclusões da dissertação com base em uma análise crítica e comparativa das fontes legais estudadas.

O estudo será estruturado em três capítulos. No primeiro capítulo, aborda-se a proteção de dados pessoais na sociedade da informação, destacando sua evolução e importância no contexto contemporâneo. A preocupação com a proteção de dados, que inicialmente emergiu nos Estados Unidos devido ao desenvolvimento econômico e tecnológico, influenciou a elaboração de regulamentos em todo o mundo. Na Europa, a Alemanha foi pioneira ao estabelecer normas na área, especialmente após a Segunda Guerra Mundial, quando a proteção de dados pessoais se tornou essencial para evitar práticas discriminatórias. Essa necessidade levou ao desenvolvimento do conceito de autodeterminação informativa, concedendo aos indivíduos o direito de controlar seus próprios dados.

O capítulo inicial também apresenta a evolução da legislação de proteção de dados em diferentes fases. A primeira geração de leis focou na regulação de bancos de dados públicos,

enquanto a segunda trouxe a necessidade de consentimento para o tratamento de dados pessoais no setor privado. Na terceira geração, destacou-se a autodeterminação informativa, consolidando o protagonismo do indivíduo no controle de seus dados. Por fim, a quarta geração buscou dinamizar o consentimento e estabeleceu a criação de autoridades independentes para fiscalizar o cumprimento das leis de proteção de dados. A União Europeia, com a adoção da Diretiva 95/46 e do Regulamento Geral de Proteção de Dados (GDPR), teve papel crucial na definição desses padrões, influenciando diretamente a LGPD brasileira.

Aborda-se, ainda, o desenvolvimento do regime jurídico de proteção de dados pessoais no Brasil. Destaca-se que, mesmo antes da LGPD, elementos de proteção já estavam presentes na legislação e na jurisprudência. O Habeas Data foi introduzido pela Constituição Federal de 1988, assegurando o direito de acesso e retificação de informações pessoais. O Marco Civil da Internet, por sua vez, estabeleceu direitos relativos à proteção de dados no ambiente digital. Além disso, o Código de Defesa do Consumidor regulamentou os cadastros e bancos de dados, estabelecendo padrões claros para a coleta e tratamento de dados dos consumidores. A LGPD, promulgada em 2018, consolidou a proteção de dados como um direito fundamental, alinhando-se aos princípios do GDPR europeu e ampliando a autonomia e controle do titular sobre seus dados.

No contexto brasileiro, também será analisado o reconhecimento da proteção de dados pessoais como um direito fundamental pelo Supremo Tribunal Federal (STF) em 2020. A decisão do STF, posteriormente reforçada pela Emenda Constitucional nº 115/2022, estabeleceu a proteção de dados como um direito intrínseco à dignidade da pessoa humana e ao livre desenvolvimento da personalidade. O reconhecimento desse direito demanda bases jurídicas claras e medidas organizacionais que garantam a segurança e transparência no tratamento de dados.

O primeiro capítulo examina ainda os desafios contemporâneos apresentados pela sociedade da informação, como o uso da inteligência artificial e do *big data* na exploração dos dados pessoais. No ambiente digital, a questão do consentimento ganhou destaque como uma ferramenta central para garantir a autodeterminação informativa. Contudo, há críticas sobre a efetividade do consentimento quando o acesso a determinados serviços ou produtos depende da aceitação de políticas de privacidade. Além disso, discute-se o conceito de "design viciante", estratégias empregadas pelas *big techs* para manter a atenção dos usuários e coletar dados de forma invasiva, gerando debates sobre privacidade e proteção dos direitos dos consumidores.

Ao final do primeiro capítulo, enfatiza-se a importância da transparência como princípio fundamental no tratamento de dados pessoais. Destaca-se a necessidade de protocolos de conformidade, a promoção de boas práticas de governança e a adoção do direito à explicação para garantir que os titulares compreendam como seus dados são processados. A transparência é essencial para equilibrar a relação entre consumidores e fornecedores, sobretudo diante das complexidades introduzidas pela inteligência artificial e o processamento de dados em larga escala.

No segundo capítulo, aborda-se o direito do consumidor à proteção de dados pessoais no contexto do comércio eletrônico e a importância do consentimento válido. Inicialmente, foram destacadas as transformações nos padrões de consumo após a Segunda Guerra Mundial, com a modernização da economia e a transição para o modelo digital. Isso resultou na intensificação das práticas de consumo, incentivadas pela mídia e pela produção em massa de bens. O reconhecimento dos direitos do consumidor como direitos fundamentais pela ONU e a subsequente elaboração do Código de Defesa do Consumidor (CDC) no Brasil ressaltaram a importância de equilibrar as relações de consumo, particularmente no ambiente digital.

O surgimento do comércio eletrônico ampliou a vulnerabilidade do consumidor, levando à necessidade de maior proteção jurídica. A nova economia digital, marcada pelo uso intensivo de dados pessoais, trouxe desafios para garantir segurança, confiabilidade e proteção das informações do consumidor. Além disso, o cenário dos contratos eletrônicos agrava questões como adulterações, fraudes e apropriação indevida de dados, elevando a vulnerabilidade informacional e técnica dos consumidores. O reconhecimento dessas vulnerabilidades é essencial para implementar uma abordagem protetiva eficaz, principalmente diante de práticas comerciais que exploram a falta de proficiência tecnológica do consumidor.

A obtenção do consentimento válido pelo titular dos dados pessoais é um elemento central na LGPD brasileira. Esse consentimento deve ser livre, informado e inequívoco, e no caso dos dados sensíveis, deve ainda ser destacado, garantindo que o consumidor tenha controle sobre a coleta e o processamento de seus dados pessoais. A legislação estabelece procedimentos claros para obtenção do consentimento, exigindo transparência e boa-fé nas práticas comerciais. A proteção de dados pessoais está vinculada ao princípio da boa-fé objetiva, que impõe ao controlador de dados o dever de garantir segurança e respeito às expectativas legítimas do consumidor.

O consentimento do titular é fundamental para o exercício da autodeterminação informativa, sendo um mecanismo que empodera o consumidor a autorizar ou negar o tratamento de seus dados. A revogação do consentimento também é um direito assegurado ao consumidor, caso ele deseje interromper o processamento de suas informações. Esse controle sobre os dados é acompanhado de outros princípios, como a proteção especial a dados sensíveis, a segurança da informação e a limitação temporal no armazenamento de dados, evitando seu uso indevido ou por tempo prolongado sem necessidade.

Além disso, a proteção dos dados pessoais é considerada um direito básico do consumidor, conforme o CDC. A necessidade de proteger a personalidade, a privacidade e os dados pessoais do consumidor reflete a importância de garantir a segurança e a lisura nas relações de consumo. Para uma proteção eficaz, é necessário um diálogo entre a LGPD e o CDC, destacando princípios como transparência, compatibilidade de finalidade, direito de acesso e revogação de consentimento, proteção aprimorada de dados sensíveis, segurança e limitação temporal dos dados.

Ao final do segundo capítulo, destaca-se a importância da colaboração entre o setor público e privado na proteção dos direitos dos consumidores. Enquanto o poder público atua como fiscalizador e defensor desses direitos, o setor privado é incentivado a adotar boas práticas e protocolos de governança para assegurar o cumprimento das obrigações relativas à proteção de dados. A Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel importante nesse processo, incentivando a conformidade e promovendo um diálogo contínuo para a proteção dos dados pessoais no contexto das relações de consumo.

Em sede do terceiro capítulo, aborda-se o conceito e os impactos dos padrões obscuros, conhecidos como "*dark patterns*", no consentimento válido para a coleta de dados pessoais. Inicialmente, destaca-se que essas práticas são estratégias de design de interface digital usadas para influenciar as decisões dos usuários sem que estejam totalmente informados e cientes de suas ações. Essas técnicas têm origem na manipulação comportamental dos consumidores desde a década de 1970 e se intensificaram no ambiente digital. A criação e a evolução dos padrões obscuros têm como objetivo explorar vulnerabilidades dos consumidores, interferindo na tomada de decisões conscientes.

O capítulo terceiro apresenta vários exemplos dessas práticas, como a adição de itens ao carrinho de compras sem o consentimento explícito do usuário, falsas táticas de escassez de produtos para induzir compras rápidas e métodos que dificultam o cancelamento de

assinaturas. Essas estratégias reduzem a autonomia dos consumidores e podem levar a decisões indesejadas ou prejudiciais. Empresas como Amazon e Facebook foram citadas como casos práticos, em que o uso de padrões obscuros prejudica a experiência do usuário ao criar barreiras para cancelar serviços ou manipular configurações de privacidade.

Além disso, foram analisados esforços regulatórios para coibir essas práticas. A legislação de proteção de dados da Califórnia e outras iniciativas nos Estados Unidos estabeleceram restrições ao uso de padrões obscuros, proibindo linguagens confusas, coleta de informações desnecessárias e táticas para desencorajar os usuários a optar por não compartilhar dados. Na Europa, as Diretrizes nº 3/2022 da EDPB classificaram e detalharam tipos de padrões obscuros, fornecendo orientações para prevenir essas práticas em plataformas digitais, especialmente em redes sociais.

O capítulo também aborda as relações entre padrões obscuros e o princípio da boa-fé objetiva (*fairness*), tanto no direito do consumidor quanto na proteção de dados pessoais. O princípio da boa-fé objetiva estabelece uma obrigação de transparência, cooperação e respeito aos interesses dos consumidores, garantindo uma conduta ética nas relações jurídicas. No contexto digital, esse princípio se estende ao design de interfaces e práticas que buscam induzir o consentimento ou manipular as escolhas dos usuários, tornando o tema relevante para a análise de padrões obscuros.

O terceiro capítulo foi concluído ressaltando a necessidade de medidas estruturais e regulamentações específicas para abordar as práticas de padrões obscuros no Brasil. Enquanto as disposições do CDC e da LGPD fornecem uma base para combater essas práticas, há uma lacuna regulatória que precisa ser preenchida com políticas claras e sanções efetivas. Além disso, destaca-se a importância de sensibilizar e educar os consumidores sobre seus direitos e as táticas manipuladoras empregadas por plataformas digitais.

Por fim, enfatiza-se a teoria de "*digital fairness by design*", inspirada em conceitos de "*privacy by design*", para prever e prevenir a adoção de padrões obscuros no design de plataformas digitais. Isso inclui adotar uma abordagem preventiva e proativa, com o objetivo de garantir que as empresas respeitem os princípios de boa-fé e transparência ao conceber suas interfaces e ao tratar os dados pessoais dos consumidores, criando um ambiente digital justo e seguro para todos os usuários.

1 A PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO

1.1 Desenvolvimento do regime jurídico de proteção de dados pessoais no Brasil: aspectos legais e constitucionais

1.1.1 *Histórico de proteção de dados pessoais até o Brasil*

A proteção de dados pessoais é um assunto em ascensão em distintas regiões e contextos, sendo uma preocupação global. Alguns dos principais institutos de proteção de dados surgiram nos Estados Unidos, apesar de terem sido tratados sob a roupagem da privacidade como sinônimo. As origens na América do Norte deram-se, sobretudo, pela ocorrência nessa região de um desenvolvimento econômico e tecnológico primevo na escala global, o que permitiu por consequência serem pioneiros também na identificação dos problemas relacionados à violação da privacidade. Isso ocasionou, por conseguinte, a necessidade de instituir um marco regulatório e jurídico para proteger de violações os direitos que estavam sob ameaça, dentre os quais se destaca o direito à privacidade[2].

Institutos que possuem especial relevância na Lei Geral de Proteção de Dados Pessoais brasileira (LGPD) e no Regulamento Geral de Proteção de Dados europeu (GDPR) tiveram origem na arquitetura regulatória formada nos Estados Unidos, como os princípios da finalidade, livre acesso, transparência e segurança[3].

Embora as raízes deste tema não estejam efetivamente na Europa, é lá que as discussões sobre a proteção de dados pessoais se aprofundaram. A Alemanha foi um dos primeiros países a estabelecer normas nessa área[4] e as regulamentações europeias têm exercido uma influência significativa na legislação brasileira nesse âmbito.

No período pós-guerra, a ideia de proteção de dados ganhou força na Europa como um meio de garantir um direito fundamental do indivíduo de ser protegido contra práticas discriminatórias. Uma das primeiras medidas nessa direção foi a legislação de Hesse (*Land de Hesse)*, na Alemanha, específica do Estado de Hesse, em 1970. Essa lei visava regular as atividades de centros de processamento de dados operados por entidades governamentais,

---

[2]DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: Tratado de Proteção de Dados Pessoais. CORRÊA, Adriana Espíndola… [et. al.]; coordenação Danilo Doneda …[et. al.]. - 2 ed. - Rio de Janeiro: Forense, 2023, p. 5.
[3]*Ibidem*, p. 5-7.
[4]DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. *In*: Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2020, p. 37.

representando assim uma lei estadual. Posteriormente, em 1977, surgiu a primeira legislação federal relativa a essa questão[5].

Naquela época, percebeu-se que muitas das terríveis ações ocorridas durante a guerra, particularmente sob o regime nazista, foram facilitadas pelo uso de dados pessoais, incluindo informações sobre crenças, cultura e orientação sexual. Estes dados foram coletados pelo Estado através de censos realizados antes do período crítico da guerra. Mais tarde, em 1983, o desafio à Lei do Censo no Tribunal Constitucional teve um papel crucial no estabelecimento do direito à autodeterminação informativa. Isso marcou o reconhecimento de um direito subjetivo e essencial do indivíduo, que passaria a ter consciência e um papel central no controle e na gestão dos seus próprios dados. Nesse cenário, a importância do livre desenvolvimento da personalidade e da privacidade como direitos fundamentais foi também enfatizada e analisada[6].

A necessidade de uma arquitetura regulatória apta a proteger os dados pessoais dos indivíduos foi se tornando cada vez mais urgente, sendo consentânea à formação do Estado Moderno. Após os idos de 1945, os Estados observaram a relevância de obter o controle dos dados pessoais dos seus cidadãos com vistas a "planejar e coordenar as suas ações para um crescimento ordenado"[7].

Atribui-se especial relevância à tecnologia para a influência desse comportamento por parte do Estado, "essencialmente a ciência computacional que revolucionou quantitativa e qualitativamente a capacidade de processamento de tais informações"[8]. Como visto, sua utilização teve influência até mesmo no processo de mapeamento do regime nazista, de modo que a criação de bancos de dados e a sua utilização para o controle da população se tornou um instrumento viável e deveras perigoso. Foi nesse contexto que se constituiu a primeira geração de leis de proteção de dados pessoais, destinadas a regular a criação de bancos de dados pelo Estado[9].

Após a tentativa de sanar a questão do manuseio de dados pessoais pela máquina administrativa com os grandes bancos de dados, a preocupação tomou outro viés, dessa vez relacionada à criação de pequenos bancos de dados, no entanto pulverizados, pela esfera

---

[5]DONEDA, 2020, p. 37.
[6]*Ibidem*, p. 37-38.
[7]BIONI, Bruno. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento.** In: Minha Biblioteca, (3rd edição). Grupo GEN, 2021, p. 109.
[8]*Ibidem*, p. 109-110.
[9]*Ibidem*, p. 110.

privada. Pelo fato de tanto o Estado quanto o particular realizarem atividades que colocam em risco o titular de dados, foi necessário o desenvolvimento de uma estratégia que transferisse a ele o controle e a responsabilidade de protegê-los, surgindo nesse contexto a figura do consentimento e marcando essa movimentação a segunda geração de leis de proteção de dados pessoais[10].

Bruno Bioni explica que, "se antes o fluxo das informações pessoais deveria ser autorizado pelo Estado, agora cabe ao próprio cidadão tal ingerência que, por meio do consentimento, estabelece as suas escolhas no tocante à coleta, uso e compartilhamento dos seus dados pessoais"[11]. O contexto de surgimento do consentimento, portanto, aponta para uma espécie de encruzilhada, em vista dos riscos oferecidos pelo Estado ao gerir os dados pessoais dos indivíduos e da preocupação com o seu uso indevido pelos entes privados.

Em 1995, a União Europeia (UE) adotou a Diretiva 95/46, estabelecendo um conjunto unificado de regras de proteção de dados para os países membros[12]. Com a evolução da internet e da tecnologia, que cada vez mais dependem de dados pessoais, surgiu a necessidade de uma regulamentação mais atualizada que abordasse questões inéditas e minimizasse os riscos para os titulares dos dados. Foi nesse contexto que, em 2012, surgiu a proposta da Regulamentação Geral de Proteção de Dados (GDPR) da União Europeia[13].

Nessa conjuntura, com os importantes avanços vistos no sentido de conferir autonomia ao indivíduo para o controle dos seus dados pessoais, os normativos foram se aprimorando de modo a ampliar o seu protagonismo. Dessa forma, "as normas de proteção de dados pessoais procuraram assegurar a participação do indivíduo sobre todos os movimentos dos seus dados pessoais: da coleta ao compartilhamento"[14]. Assim, ganhou destaque a figura da autodeterminação informativa, instituto que habilita o titular a um controle extensivo sobre os dados pessoais, e isso marca a terceira geração de leis de proteção de dados pessoais[15].

A GDPR destaca-se por sua aplicabilidade extraterritorial, regulando o tratamento de dados pessoais de cidadãos da UE ou de dados localizados na UE, independentemente de onde o controlador ou processador esteja sediado. Contudo, a GDPR não confere aos indivíduos a

[10]BIONI, 2021, p. 111.
[11]*Ibidem*, p. 111.
[12]LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Européia (LGPD e GDPR) e seus respectivos instrumentos de *Enforcement*. In: **Revista do programa de Direito da União Européia**. FGV: Rio de Janeiro, 2021, p. 41.
[13]*Ibidem*, p. 41.
[14]BIONI, *op. cit.*, p. 111.
[15]*Ibidem*, p. 111.

propriedade de seus dados, mas sim o controle sobre o uso, armazenamento e compartilhamento desses dados. Inclui o direito de solicitar a exclusão dos dados e de ser informado de forma transparente sobre todas as operações realizadas com eles[16].

Essa abrangência extraterritorial é crucial para proteger os cidadãos da UE de violações por parte de empresas localizadas em países com leis diferentes ou sem regulamentação específica sobre proteção de dados. Assim, a aplicação extraterritorial da GDPR representa um direito fundamental e supranacional à proteção de dados[17].

A evolução das legislações de proteção de dados pessoais seguiu uma trajetória marcada por importantes marcos ao longo do tempo. A primeira geração de leis focou na regulação dos bancos de dados públicos, enquanto a segunda estabeleceu o consentimento como princípio fundamental para o tratamento de dados pessoais. Posteriormente, a terceira geração avançou para a autodeterminação informativa, que consolidou o direito dos indivíduos de controlarem suas informações. No entanto, esses avanços não ocorreram de forma harmônica ou linear, evidenciando desafios e dilemas ao longo de sua implementação.

Bioni[18] ressalta que a centralidade do consentimento como mecanismo de proteção de dados trouxe consigo uma série de complicações. Desde a segunda geração de leis, questionava-se a efetividade de um modelo centrado no poder de escolha do indivíduo, considerando que diversas relações sociais tinham como condição a entrega de dados pessoais para sua realização. Exemplos disso incluem burocracias governamentais, o exercício do direito ao voto e o acesso a bens de consumo, como serviços bancários, em que a disponibilização de dados pessoais era uma exigência para a participação nessas atividades. Esse contexto evidenciou as limitações de uma abordagem baseada exclusivamente no consentimento, apontando para a necessidade de uma proteção de dados mais abrangente e equilibrada na sociedade contemporânea.

Por essa razão, a quarta geração de leis de proteção de dados pessoais veio como uma tentativa de dinamizar a questão do consentimento, que ficou prevista de modo deficitário nos marcos normativos anteriores. Assim, Bioni[19] explica que a quarta geração de normas é marcada pela propagação de autoridades independentes, incumbidas de zelar pela aplicação das leis de proteção de dados pessoais, somada às normas que relativizam a centralidade do

[16]LORENZON, 2021, p. 43-44.
[17]*Ibidem*, p. 44.
[18]BIONI, 2021, p. 112.
[19]BIONI, 2021, p. 112.

consentimento do titular, que ocorreu com a delimitação dos dados pessoais sensíveis cujo titular não tem margem de escolha estritamente livre quanto ao processamento.

A criação de uma autoridade de proteção de dados é apontada pela literatura como um elemento fundamental para assegurar a efetividade dos direitos dos cidadãos no que concerne ao tratamento de seus dados pessoais. Uma autoridade competente e especializada possibilita a implementação de mecanismos eficazes para garantir esses direitos e, além disso, facilita a adaptação do setor privado ao marco regulatório de proteção de dados. Diferentemente dos tribunais, que se manifestam em situações específicas de conflito, a autoridade tem o papel de construir padrões de aplicação da lei e fornecer orientações consistentes sobre o tema[20]. Dessa forma, sua presença contribui para uma maior segurança jurídica e promove um ambiente regulatório claro e transparente.

Outro ponto crucial é a independência dessa autoridade. Para que ela possa atuar de forma imparcial e eficaz, é necessário que suas atividades de fiscalização, aplicação de sanções e decisões não estejam sujeitas a qualquer tipo de hierarquia ou influência externa. A independência também é reforçada pelo mandato dos membros com poder decisório, garantindo que suas funções sejam desempenhadas sem riscos de interferência política e de maneira técnica. Esse aspecto é considerado fundamental para que a autoridade desempenhe seu papel de forma autônoma e confiável. Nesse sentido, a LGPD, em sua versão original aprovada pelo Congresso Nacional brasileiro, estabeleceu que a Autoridade Nacional de Proteção de Dados (ANPD) deveria ter a natureza de autarquia especial, assegurando sua autonomia funcional e decisória[21].

A independência e autonomia da autoridade de proteção de dados são, portanto, elementos essenciais para que ela possa atuar com eficácia tanto na proteção dos direitos dos titulares de dados quanto no apoio ao setor privado na conformidade com a legislação. Uma autoridade independente não apenas garante uma abordagem técnica e imparcial na aplicação da lei, mas também reforça a confiança de cidadãos e empresas no sistema regulatório. Ao assegurar que suas atividades sejam conduzidas sem hierarquias ou interferências externas, a autoridade fortalece a credibilidade do marco legal de proteção de dados e possibilita um ambiente mais seguro e eficiente para o tratamento de informações pessoais.

---

[20]MENDES, Laura Schertel Ferreira. BIONI, Bruno Ricardo. O Regulamento europeu de proteção de dados pessoais e a Lei Geral de Proteção de Dados brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**: São Paulo, 2019, p. 14.

[21]*Ibidem*, p. 14.

Portanto, é incontestável que a autonomia e independência da autoridade de proteção de dados são fundamentais para sua eficácia no território onde atua. Sua vinculação ao governo pode comprometer sua eficiência, como já mencionado, sendo que por essa razão a ANPD, no Brasil, deixou de ser vinculada à presidência da república para assumir o regime de autarquia especial, com estrutura muito semelhante à de uma agência reguladora federal, conforme determinado pela LGPD. Além disso, é vital reconhecer que o Estado está sujeito à LGPD, não estando acima dela, e deve obedecer integralmente às suas diretrizes no que tange ao respeito aos direitos dos titulares dos dados.

Mendes e Bioni[22] também destacam que a independência da autoridade de proteção de dados pode trazer benefícios econômicos e políticos significativos para o país. Tais benefícios incluem desde a adesão do Brasil à Organização para a Cooperação e Desenvolvimento Econômico (OCDE) até a conquista da adequação europeia, melhorando as relações comerciais com outros países. Isso se deve ao fato de que a independência da autoridade nacional de proteção de dados aumenta a segurança no tráfego de dados, promovendo maior confiança internacional de que os dados dos cidadãos serão respeitados e protegidos de violações de forma rigorosa e ética, sem interferência do Estado, que pode ter interesses próprios no uso dos dados no âmbito da economia digital.

A GDPR não só influenciou a criação da Lei Brasileira de Proteção de Dados Pessoais, mas também serviu como um alicerce principiológico na fundamentação de decisões judiciais no Brasil. Isso ocorre através da adoção do direito comparado, um método que busca em legislações, como a europeia, ferramentas e técnicas que auxiliam na fundamentação de decisões judiciais e na resolução de questões não abordadas pela legislação brasileira. Este procedimento tem apoio legal no art. 4° da Lei de Introdução às normas do Direito Brasileiro, que permite ao juiz basear suas decisões na analogia, nos costumes e nos princípios gerais de direito. Vale destacar que o Supremo Tribunal de Justiça (STJ) possui autoridade para homologar sentenças estrangeiras, conforme estabelecido no art. 105, I, “i” da Constituição Federal[23], possibilitando a integração de decisões baseadas em legislações estrangeiras no direito brasileiro.

A regulação do fluxo internacional de dados ganhou importância significativa no cenário global, especialmente no âmbito da OCDE. Os países membros foram pressionados a

[22]MENDES; BIONI, 2019, p. 15.

[23]BRASIL. **Constituição Federal de 5 de outubro de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm. Acesso em: 20 mai. 2023. (n.p.)

estabelecer regimes jurídicos que possibilitassem o controle desse fluxo, assegurando a proteção de dados pessoais além de suas fronteiras. Nesse contexto, a falta de incorporação de padrões internacionais de proteção poderia resultar na exclusão de um país ou bloco econômico do mapa global de livre fluxo de dados, prejudicando suas relações comerciais e sua posição na economia digital[24].

Diante desse cenário, as legislações nacionais e regionais que surgiram para regular o tratamento de dados passaram a incluir regras rígidas sobre a transferência internacional de informações. Essas normas visam garantir que, ao transitar de um país para outro, os dados pessoais estejam submetidos a níveis adequados de proteção. Dessa forma, o país destinatário deve possuir um sistema de proteção de dados equivalente ao país de origem para que a transferência seja considerada legal. Essa abordagem busca manter um padrão de segurança global e evitar que dados pessoais sejam transferidos para jurisdições que ofereçam proteção insuficiente[25].

A implementação de tais regras impacta diretamente o fluxo de informações e a integração econômica entre diferentes países e blocos regionais. Ao exigir equivalência no nível de proteção de dados, cria-se um incentivo para que nações harmonizem suas legislações com padrões internacionais, facilitando a troca segura de informações e a cooperação transfronteiriça. No entanto, essas exigências também geram desafios para países que ainda não desenvolveram marcos legais robustos, os quais correm o risco de ficarem isolados no contexto global de circulação de dados, evidenciando a necessidade de um esforço internacional coordenado para estabelecer padrões de proteção que sejam aceitos e reconhecidos amplamente.

Portanto, é possível afirmar que a estruturação institucional para a regulamentação de dados no Brasil ocorreu em grande medida devido à necessidade de alinhamento com as normas já estabelecidas na União Europeia e em outros países com os quais o Brasil mantém relações comerciais, além da busca notável de ingressar na OCDE. Esse processo de adoção de modelos europeus foi largamente impulsionado pela necessidade de conformidade com as normativas internacionais, considerando também o crescente entrelaçamento global no mercado e a interdependência entre os países no novo cenário do mercado digital. Esta interconexão e constante interação resultam na transferência massiva de dados pessoais,

[24]MENDES; BIONI, 2019, p. 3.
[25]*Ibidem*, p. 3.

especialmente de consumidores que adquirem produtos de empresas internacionais, fazendo da regulamentação de proteção de dados uma urgência.

A harmonização das normativas de proteção de dados é uma exigência da crescente interconexão global, particularmente no âmbito do comércio digital, em que o uso e processamento de dados pessoais ocorrem de forma intensa e rápida. Nesse contexto, a equivalência entre a Lei Geral de Proteção de Dados brasileira e o Regulamento Geral de Proteção de Dados europeu está se tornando cada vez mais relevante, dada a necessidade de estabelecer padrões comuns que favoreçam o livre fluxo de dados entre países. Segundo Mendes e Bioni[26], essa equivalência é fundamental para o Brasil em pelo menos dois aspectos, visando tanto a adequação à legislação europeia quanto o estabelecimento de critérios próprios de análise de conformidade de normas estrangeiras.

O primeiro motivo para essa harmonização, conforme explicado pelos autores, é a potencialidade de o Brasil ser reconhecido como um país "adequado" pelo sistema europeu de proteção de dados. Esse reconhecimento seria formalizado por meio de uma decisão favorável da Comissão Europeia, que avaliaria se o nível de proteção oferecido pela LGPD é equivalente ao do GDPR. Caso essa adequação seja confirmada, seria uma vantagem significativa para as entidades públicas e privadas brasileiras, pois facilitaria o tratamento e a transferência de dados entre o Brasil e a União Europeia, impulsionando a cooperação comercial e tecnológica. Assim, a convergência entre as normas europeias e brasileiras pode contribuir para uma maior integração do Brasil ao padrão de conformidade da União Europeia, fortalecendo laços comerciais e beneficiando economicamente ambas as regiões[27].

O segundo motivo destacado por Mendes e Bioni[28] diz respeito à necessidade de o Brasil desenvolver seus próprios critérios para avaliar a adequação de normas estrangeiras à LGPD, conforme o previsto no artigo 33, inciso I, da lei brasileira. Essa disposição legal impõe que a transferência internacional de dados só pode ocorrer se o país de destino garantir um nível de proteção compatível com o da LGPD. Além disso, o artigo 34 da LGPD atribui à ANPD a competência para avaliar o grau de adequação das legislações de países estrangeiros. Na análise de compatibilidade, serão considerados fatores como as normas gerais e setoriais do país de destino, a natureza dos dados tratados, a observância de princípios e direitos de

[26]MENDES; BIONI, 2019, p. 15.
[27]*Ibidem*, p. 15.
[28]*Ibidem*, p. 15.

proteção de dados, bem como a existência de garantias judiciais e institucionais para proteger esses direitos.

Logo, a harmonização entre a LGPD e o GDPR é uma via de mão dupla: não apenas é fundamental para que o Brasil alcance um status de adequação perante a União Europeia, mas também é necessária para que o país desenvolva critérios próprios e robustos de avaliação de normas estrangeiras, assegurando um nível de proteção adequado na transferência internacional de dados. Dessa forma, a busca por equivalência entre as legislações favorece a segurança jurídica nas transações comerciais e a proteção de dados pessoais, além de reforçar a posição do Brasil como ator relevante no cenário global de proteção de dados, promovendo uma regulamentação que seja tanto nacional quanto alinhada aos padrões internacionais[29].

Da mesma forma, o Brasil deve examinar as semelhanças entre suas leis e as legislações estrangeiras para possibilitar a continuidade e o desenvolvimento de acordos e relações comerciais. Isso implica na análise da compatibilidade da legislação externa, incluindo a GDPR, com a LGPD nacional.

A criação da Lei Geral de Proteção de Dados Pessoais brasileira foi fortemente influenciada pelo Regulamento Geral de Proteção de Dados da União Europeia, como já mencionado anteriormente. Contudo, antes da LGPD, já existiam elementos e proteções específicas para os dados pessoais na legislação e na jurisprudência brasileiras.

No campo da jurisprudência, desde a década de 90, pode-se observar casos demonstrando a incorporação da proteção à privacidade. Acerca do tema, Mendes[30] relembra um julgamento notável de Habeas Data pelo STF, que debateu o direito de um indivíduo de acessar informações armazenadas pelo extinto Serviço Nacional de Informações (SNI). A análise focou no reconhecimento, pelos ministros, do direito material de acesso a dados pessoais, relacionando-o aos direitos da personalidade, à intimidade e à autonomia individual.

Fica evidente que, no pensamento do judiciário brasileiro, mesmo antes da implementação de regulamentações específicas como a Lei do Marco Civil da Internet e, posteriormente, a LGPD, já existia um direito material à proteção de dados, entendida como intrinsecamente ligada à personalidade e à privacidade.

---

[29]MENDES; BIONI, 2019, p. 15.

[30]MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental.** Ed. Saraiva: São Paulo, 2014.

Segundo Doneda[31], já existia no Brasil uma estrutura regulatória que, mesmo não nomeando explicitamente a "proteção de dados", garantia ao indivíduo proteção contra violações de seus dados. Isso se dava principalmente através da salvaguarda da privacidade e da implementação de princípios de direito do consumidor, além de estar vinculado à proteção das liberdades individuais. Assim, o termo "proteção de dados" só foi recentemente incorporado, dentro de uma organização de princípios. Doneda também enfatiza a relevância do tema da privacidade na adoção do direito à proteção de dados no Brasil, devido à sua forte associação.

A Constituição Federal de 1988 introduziu o Habeas Data como um instrumento constitucional (art. 5º, LXXII)[32], assegurando o direito constitucional do titular dos dados de acessar informações detidas pelo Poder Público e por entidades privadas, bem como o direito de retificar essas informações. Isso estabeleceu a base para o direito do titular dos dados de saber quais dados pessoais estão sob a posse do controlador, ainda que naquele momento a tutela estivesse mais atrelada à privacidade do que aos dados em si.

O Marco Civil da Internet (Lei nº 12.965/2014) define os direitos e garantias dos usuários na internet. Em seu art. 7º, estabelece direitos relacionados à proteção da intimidade e da vida privada (art. 7º, I), ao sigilo das comunicações pela internet e das informações armazenadas (art. 7º, II e III), entre outros direitos e garantias. Portanto, mesmo antes da LGPD, o Brasil já possuía uma legislação específica sobre proteção de dados pessoais, focada na defesa do indivíduo na internet. Esta legislação apresenta várias convergências com a LGPD e reforça a necessidade de tal regulamentação[33].

O Marco Civil da Internet trouxe importantes diretrizes para a proteção de dados pessoais, especialmente ao abordar a autodeterminação informacional e o consentimento do titular dos dados. A legislação estabelece que o titular dos dados deve ser claramente informado sobre os processos de coleta, uso, armazenamento e tratamento de seus dados, conforme disposto no art. 7º, inciso VIII. Os dados pessoais devem ser utilizados para finalidades legítimas e claramente especificadas nos termos de uso, garantindo que o tratamento das informações seja transparente e respeite os direitos do titular. Dessa forma, o

[31]DONEDA, 2020.
[32]BRASIL. **Constituição Federal de 5 de outubro de 1988.** (n.p.)
[33]BRASIL. **Lei nº 12.965, de 23 de abril de 2014. Lei do Marco Civil da Internet.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 mai. 2023. (n.p.)

Marco Civil promove a responsabilidade na gestão de dados pessoais, exigindo que qualquer coleta ou processamento seja feito de maneira explícita e informada[34].

O consentimento é um aspecto central dessa regulamentação, sendo necessário que ele seja expresso e destacado, conforme prevê o art. 7º, inciso IX. Isso significa que o consentimento geral fornecido ao aceitar os termos de uso e políticas de privacidade não é suficiente, é preciso que o tratamento de dados pessoais seja autorizado em uma janela específica, de modo a garantir que o usuário tenha ciência do que está autorizando e possa revogar essa permissão a qualquer momento, sem perder o acesso ao serviço. Essa exigência reforça a importância da autonomia do titular dos dados, permitindo que ele mantenha o controle sobre suas informações pessoais e sobre a relação estabelecida com a entidade que realiza o tratamento desses dados. Dessa maneira, o Marco Civil busca equilibrar a proteção da privacidade do usuário com o funcionamento das atividades econômicas digitais[35].

Observa-se que, já com o Marco Civil da Internet, a importância do consentimento na proteção de dados do titular é evidente. A exigência de que o consentimento seja inequívoco, ou seja, extremamente claro e específico, reflete a preocupação com o conhecimento do titular sobre o uso e o destino de seus dados. Além disso, ao possibilitar a revogação do consentimento, o titular é empoderado sobre seus dados, podendo-se afirmar que isso estabelece um direito de controle sobre eles.

O CDC pode ser considerado o primeiro normativo a tratar da proteção de dados no Brasil. Segundo Mendes[36], o CDC foi pioneiro ao prever normas específicas relacionadas ao tratamento de dados pessoais, principalmente no que diz respeito aos cadastros e bancos de dados de consumo. O artigo 43, em particular, introduziu regras que estabeleceram parâmetros claros para o funcionamento desses cadastros, garantindo transparência e direitos ao consumidor no que se refere ao tratamento de suas informações. Desse modo, o CDC lançou as bases para a regulamentação e proteção de dados no país, influenciando a evolução subsequente dessa área do direito. É importante esclarecer que não há um conflito entre

---

[34]SILVA, Alexandre Assunção. A proteção pelo MPF dos dados pessoais dos usuários da internet. In: BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 3. **Sistema brasileiro de proteção e acesso a dados pessoais: Análise de dispositivos da Lei de acesso à informação, da Lei de identificação civil, da Lei do marco civil da internet e da Lei nacional de proteção de dados** - Brasília: MPF, 85p. - (Roteiro de Atuação; v. 3), 2019. Disponível em: http://hdl.handle.net/11549/189803. Acesso em: 28 abr. 2023. 2019, p. 61-62.

[35]*Ibidem*, p. 61-62.

[36]MENDES, Laura Schertel Ferreira. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. São Paulo: **Revista dos Tribunais**, 2016, p. 3.

normas, mas, segundo a autora, de um diálogo entre as fontes legislativas, visando beneficiar o consumidor com a aplicação simultânea de ambas as leis[37].

A Lei nº 13.709, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 14 de agosto de 2018, com partes em vigor desde 28 de dezembro de 2018 e outras a partir de 14 de agosto de 2020, e com previsão de vigência de mais artigos a partir de 1º de agosto de 2021, estabelece um novo marco nos direitos individuais no Brasil. As diversas datas de vigência indicam os desafios enfrentados pelos profissionais para se adaptarem às normas. Também é relevante mencionar que as penalidades para violações de dados pessoais foram adiadas várias vezes e atualmente aguardam a entrada em vigor em agosto de 2021, três anos após a publicação da lei, conforme estipula o art. 65, I.

Em termos estruturais, a LGPD é uma lei relativamente concisa, com 65 artigos, abrangendo desde conceitos básicos até sanções por violação dos direitos dos titulares de dados. Com influências significativas da GDPR, a LGPD representa um avanço importante no contexto do direito do consumidor e na legislação brasileira como um todo, ao consagrar a proteção de dados pessoais como um direito individual.

Embora a LGPD não seja uma novidade absoluta no tema de proteção de dados, ela introduziu novos parâmetros e expandiu o escopo de proteção. Diferentemente da Lei do Marco Civil da Internet, que se limitava ao ambiente online, a LGPD engloba todas as formas de coleta e armazenamento de dados, tanto em meios físicos quanto digitais.

No que diz respeito ao objeto da LGPD, o art. 1º atesta:

> Art. 1º. Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.[38]

Quanto ao tratamento dos dados pessoais, o inciso X do art. 5º da LGPD categoriza:

> Art. 5º Para os fins desta Lei, considera-se:
>
> [...]
>
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento,

[37]MENDES, 2016, p. 3.

[38]BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mai. 2023. (n.p.)

> eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.[39]

A definição ampla do que constitui 'tratamento' de dados foi crucial para esclarecer as ações abrangidas pela legislação, evitando incertezas entre os operadores do direito. Maldonado[40] destacou a importância dessa abrangência, que inclui todas as operações relacionadas aos dados pessoais, desde a coleta até a sua eliminação final. Nesse sentido, até mesmo o simples armazenamento é considerado tratamento, conforme estabelecido na norma, implicando que a posse de dados pessoais exige a observância da legislação. O autor também ressalta que, embora a proteção de dados seja frequentemente associada ao ambiente digital, a lei também protege dados coletados e armazenados fisicamente, proporcionando a eles a mesma proteção.

O artigo 4º da Lei exclui algumas formas de tratamento, mas isso não implica isenção da observância de protocolos ou liberdade no uso de dados pessoais. De acordo com Maldonado[41], todos que usam ou tratam dados pessoais estão sujeitos à legislação, com o objetivo de abranger todos os agentes de tratamento. Isso significa que, uma vez que a atividade se enquadre na definição legal, ela se aplica a todos os indivíduos envolvidos em qualquer uma das operações descritas no art. 5º, X. Assim, surge a obrigação de seguir as disposições sobre proteção de dados pessoais em todas as operações que envolvam dados pessoais dentro de uma organização.

1.1.2 *A proteção de dados pessoais como um novo direito fundamental no Brasil*

Em 2020, o Supremo Tribunal Federal (STF) formou maioria para reconhecer a proteção de dados pessoais como um direito fundamental. Isso ocorreu durante o julgamento de cinco Ações Diretas de Inconstitucionalidade (ADIs 6.387, 6.388, 6.389, 6.390 e 6.393), resultando na suspensão do artigo 2º da Medida Provisória 954/2020. Esta MP determinava que as empresas de telecomunicações compartilhassem com o Instituto Brasileiro de

[39]BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. (n.p.)

[40]MALDONADO, Viviane Nóbrega. **Contextualização da proteção de dados no Brasil e no mundo e elementos essenciais da LGPD.** In: Manual do DPO. São Paulo: Thomson Reuters Brasil, 2021, p. 18.

[41]*Ibidem*, p. 16.

Geografia e Estatística (IBGE) dados como nome, número de telefone e endereço de seus consumidores de telefonia móvel e fixa[42].

Foi nesse contexto que o STF expandiu a proteção de dados pessoais, considerando tuteláveis aqueles dados que são capazes de "identificar seu titular, até mesmo formando, no ambiente virtual, perfis sobre a pessoa, sem a sua participação"[43].

Portanto, Mendes e Fonseca[44] argumentam que o reconhecimento da proteção de dados pessoais como um direito fundamental, conforme evidenciado em vários votos proferidos pelo STF nos julgamentos das ADIs mencionadas anteriormente, representa um avanço significativo para a proteção constitucional dos dados pessoais no Brasil. No entanto, ainda será necessário definir mais claramente seus limites e implicações, o que poderá ser realizado tanto pela doutrina quanto pela jurisprudência. Sem a intenção de esgotar o assunto, mas visando contribuir para esta discussão, duas questões primordiais são identificadas: (i) qual é o escopo de proteção deste direito e (ii) quais são as implicações dessa proteção. Além disso, é importante salientar que, apesar de ser denominada "proteção de dados pessoais", o foco real é a proteção do titular dos dados, pois é ele que a legislação e o direito visam salvaguardar.

Seguindo essa argumentação, os autores afirmam que, consoante destacado pelo STF, qualquer limitação a esse direito fundamental, em um caso específico, requer uma base jurídica sólida e clara, acompanhada de medidas organizacionais e preventivas mínimas para assegurar a segurança dos cidadãos envolvidos e reduzir os riscos à sua personalidade. De fato, quanto mais severa for a restrição ou limitação, mais robustas devem ser as justificativas, critérios e precauções adotadas, para evitar a legitimação de intervenções na vida privada dos cidadãos em nome de objetivos genéricos ou necessidades coletivas abstratas[45].

Os autores concluem que a decisão histórica do Supremo Tribunal Federal destaca que, em um Estado Democrático de Direito, não se pode conceder carta branca a instituições públicas ou privadas, independentemente do respeito que mereçam ou da nobreza de seus propósitos. O acesso extenso aos dados pessoais dos cidadãos brasileiros requer, no mínimo,

---

[42]MENDES, Laura Schertel. FONSECA, Gabriel C. Soares da. STF reconhece direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor** | vol. 130/2020 | p. 471 - 478 | Jul - Ago / 2020. Disponível em: https://www.researchgate.net/publication/344381892_STF_reconhece_direito_fundamental_a_protecao_de_dados. Acesso em: 23 de jul. 2023. 2020, p. 1.

[43]*Ibidem*, p. 2.

[44]*Ibidem*, p. 3.

[45]MENDES; FONSECA, 2020, p. 4.

diretrizes jurídicas claras e seguras sobre essa coleta ou transferência, incluindo a previsão de medidas de segurança e critérios de intervenção que sejam proporcionais à gravidade da restrição a esse direito fundamental[46].

Em concordância com a classificação dos dados pessoais como direito fundamental pelo STF, a Emenda Constitucional nº 115/2022, aprovada em 10 de fevereiro de 2022, adicionou o inciso LXXIX ao art. 5º da Constituição, estabelecendo que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais"[47].

A elevação de status do direito à proteção de dados pessoais apresenta contornos positivos, conforme assevera Sarlet:

> Mesmo que se pudesse, como já o fizera o STF, reconhecer a proteção de dados como um direito fundamental implícito, daí extraindo todas as consequências atinentes à tal condição, o fato é que sua positivação formal, em sendo o caso, carrega consigo uma carga positiva adicional, ou seja, agrega (ou, ao menos, assim o deveria) valor positivo substancial em relação ao atual estado da arte no Brasil.[48]

Com essa abordagem, a proteção de dados pessoais obteve um nível específico de salvaguarda, facilitando significativamente a implementação efetiva de sua tutela e a repressão de práticas abusivas, em virtude do robusto sistema de proteção agora associado a este direito.

No entanto, ainda há um longo caminho a percorrer no cenário atual para garantir essa proteção de forma eficaz, especialmente diante das novas dificuldades apresentadas pelo uso da Inteligência Artificial e outras tecnologias que empregam *Big Data* em seus processos. Nos próximos anos, surgirão diversos desafios para manter em equilíbrio o avanço tecnológico e a inovação, sem que isso resulte em interferências ou violações dos direitos fundamentais.

1.2 A autodeterminação informativa no contexto da proteção de dados pessoais

Como visto, a proteção de dados pessoais passou por um extenso período de construção e consolidação, desde normas incipientes que ofereciam um regramento mínimo à tutela da personalidade, até a consolidação de uma legislação protetiva própria, como ocorreu com a LGPD, e mais tarde com a consagração da proteção de dados pessoais como

---

[46]MENDES; FONSECA, 2020, p. 4.

[47]SARLET, Ingo Wolfgang. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental. Conjur, 2022.** Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental. Acesso em: 29 jul. 2023.

[48]*Ibidem*.

um direito fundamental no cerne constitucional. A vulnerabilidade do indivíduo diante do controle e tratamento de dados pessoais, a que é condicionado cotidianamente, tornou imprescindível a construção de uma estrutura defensiva propositiva, no sentido de tutelar de forma eficiente a sua personalidade, pelos dados pessoais, que em muitos casos são explorados deliberadamente.

A autodeterminação informativa surge nesse contexto, como uma garantia de que o indivíduo terá conhecimento, com precisão, sobre o que ocorre com os seus dados pessoais, passando a ter o controle do que ocorre com eles. Isto é, o termo se refere ao controle que o indivíduo tem sobre os seus dados, de modo a autorizar ou não que eles sejam tratados e disseminados. Ela se propõe a colocar o indivíduo no centro das decisões relacionadas ao tratamento de seus dados pessoais. Esse direito busca garantir que cada pessoa tenha o poder de controlar quem tem acesso às suas informações e com que finalidade elas são utilizadas[49].

A autodeterminação informativa, além de ocupar posição de destaque no ordenamento jurídico internacional em matéria de dados pessoais, é um dos fundamentos da LGPD brasileira[50]. Nota-se, no inciso II do art. 2º da LGPD a seguinte redação: "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] II - a autodeterminação informativa"[51]. Consoante sua importante função na legislação pátria, encontra correspondência sobretudo na consagração dos direitos da personalidade.

Mendes[52] explica que as suas bases fundamentais remontam ao Tribunal Constitucional Alemão que, em 1983, quando do julgamento sobre o recenseamento da população, consolidou jurisprudência que representou um marco no desenvolvimento da proteção de dados. Naquele contexto, estava sendo questionada a constitucionalidade da lei que dispunha sobre "o recenseamento da população, das profissões, das residências e dos locais de trabalho"[53].

Na decisão, o Tribunal Constitucional Alemão reconheceu a necessidade de adaptação da interpretação dos direitos fundamentais diante do avanço das tecnologias de processamento de informações. Combinando o artigo 2º, § 1º, da Lei Fundamental (LF), que trata do livre

---

[49]DE SOUSA, Rosilene Paiva Marinho; DA SILVA, Paulo Henrique Tavares. Proteção de dados pessoais e os contornos da autodeterminação informativa. **Informação & Sociedade**, v. 30, n. 2, 2020, p. 11.
[50]MENDES, 2020.
[51]BRASIL, **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**.
[52]MENDES, *op. cit.*
[53]MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 12, n. 39, p. 185-216, 2018, p. 187.

desenvolvimento da personalidade, com o artigo 1º, § 1º, que versa sobre a dignidade humana, o Tribunal formulou o conceito de autodeterminação informativa. Esse direito, segundo a Corte, confere ao indivíduo o poder de decidir sobre a coleta e o uso de seus dados pessoais, em resposta ao crescente risco representado pelo processamento automatizado de dados, que permitia o armazenamento e transmissão em larga escala de informações sem controle adequado por parte dos cidadãos[54].

A decisão também refletiu um deslocamento da proteção da privacidade baseada na esfera íntima para uma abordagem mais ampla, centrada no controle individual sobre dados pessoais, independentemente de seu caráter íntimo ou público. O Tribunal argumentou que a coleta automatizada de dados poderia criar um perfil completo da personalidade, reduzindo o poder do indivíduo de decidir livremente sobre sua vida e comportamento. Esse reconhecimento levou à formulação do direito à autodeterminação informativa como uma extensão da proteção da personalidade, capaz de oferecer maior flexibilidade na proteção dos cidadãos contra abusos no tratamento de dados. Além disso, a sentença evidenciou a necessidade de limitar o uso de dados pessoais a interesses públicos justificados, com base em leis claras e proporcionais, fortalecendo assim a proteção dos dados no contexto das sociedades digitais[55].

Antes da consagração da proteção de dados pessoais como um direito fundamental, pairavam no STF discussões referentes aos instrumentos processuais aptos para a tutela do direito do indivíduo aos dados pessoais. Uma das discussões existentes na corte era quanto ao cabimento ou não do habeas data para essa defesa. Nota-se, no entanto, que não havia uma unanimidade entre os Ministros quanto ao tema, pois à época entendia-se que não havia uma proteção constitucional específica sobre os dados pessoais, o que havia era uma proteção do direito à garantia do sigilo das comunicações previsto no art. 5º, inciso XII, da CF, e que essa tutela alcançava apenas a comunicação de dados[56].

Quando do julgamento do Recurso Extraordinário nº 673.707 MG, em 2017, cuja relatoria foi do Ministro Fux, a discussão quanto à proteção específica aos dados capazes de identificar e caracterizar um indivíduo, isto é, os dados pessoais, ganhou uma nova dimensão. O caso, de matriz tributária, versava sobre a possibilidade de acesso do contribuinte a um sistema da Receita Federal do Brasil, no qual foi impetrado um habeas data, mas o TRF 1

[54]MENDES, 2018.
[55]*Idem*, 2020.
[56]MENDES, 2018, p. 197.

havia entendido em sentido diverso, aduzindo que a Fazenda Pública não teria o dever de disponibilizar esse tipo de informação por ser complexa, onerosa e por não ter caráter público[57].

No voto, o STF sedimentou entendimento de maior amplitude à aplicação do habeas data, de modo que ele possa abranger arquivos em sentido geral, banco ou registro de dados, isto é, tudo que tenha relação ao interessado de modo direto ou indireto. Assim, o voto do Min. Relator enfatizou que as informações do contribuinte não são de uso privativo de órgãos públicos, sendo um direito da pessoa o acesso a elas, justamente por dizerem respeito ao próprio contribuinte[58]. Ao analisar o julgado, Mendes explica que:

> A importância do referido trecho reside no reconhecimento de que as informações pessoais, armazenadas e processadas por outras entidades, – pelo simples fato de possibilitarem a identificação de determinado indivíduo –, podem afetar a sua esfera de direitos e, por isso, merecem a tutela constitucional a partir da garantia do habeas data. Isto é, o julgamento acabou por extrair da garantia constitucional do habeas data também um direito material à autodeterminação informativa[59].

Na percepção da autora[60], o *habeas data* e a autodeterminação informativa possuem especial relação, na medida em que o primeiro remete à "garantia processual de proteção das liberdades e da personalidade frente ao tratamento de dados", e o segundo trata-se de um "direito material propriamente dito, que protege o indivíduo dos riscos decorrentes deste processamento". Há de se observar, portanto, que a proteção de dados pessoais como um direito fundamental nada mais é do que a garantia da autodeterminação informativa, sendo essa última a terminologia utilizada no direito alemão sobre o tema[61].

Após o reconhecimento do direito fundamental à proteção de dados pessoais na jurisprudência, logo houve a Emenda à Constituição positivando-o, conforme detalhado no primeiro tópico deste capítulo. A privacidade, nesse contexto, é vista como um aspecto essencial do desenvolvimento da personalidade, estando diretamente ligada à liberdade individual. Na percepção da literatura, é função do Estado assegurar que os cidadãos possam exercer esse direito de maneira eficaz, implementando mecanismos de proteção que garantam a transparência e a segurança no tratamento de dados. Nesse sentido, é mister a consolidação de uma estrutura robusta de regulação em matéria de dados pessoais, respaldada por políticas

---

[57] MENDES, 2018, p. 197.
[58] *Ibidem*, p. 197.
[59] *Ibidem*, p. 198.
[60] *Ibidem*, p. 198.
[61] *Ibidem*, p. 198.

públicas que promovam o respeito à privacidade e ao controle individual sobre as informações pessoais[62].

Ainda quanto à autodeterminação informativa, é importante mencionar que está estreitamente ligada ao princípio da dignidade da pessoa humana, conforme explica Sarlet, pois "se manifesta, tanto pela vinculação com a noção de autonomia, quanto com a do livre desenvolvimento da personalidade e de direitos especiais de personalidade conexos, de tal sorte que a proteção dos dados pessoais envolve também a salvaguarda da possibilidade concreta de tal desenvolvimento"[63]. Ela diz respeito também à gerência que o indivíduo possui sobre os seus dados pessoais, denominada de controle[64]. É de se notar, portanto, que a autodeterminação informativa se concretiza a partir do consentimento, por ser este um instrumento de efetivação daquele[65].

Justamente por possuir estreita relação com o consentimento é que a autodeterminação informativa também se relaciona com a autonomia privada[66]. Isto é, para que se concretize no mundo dos fatos, e o titular de dados exerça a sua autodeterminação informativa, aqui entendida como o controle sobre os dados, é essencial o elemento volitivo, qual seja, a manifestação de vontade do titular. Esse processo de exteriorização da vontade é instrumentalizado pelo consentimento, que será melhor detalhado no capítulo seguinte, mas aqui, para fins de compreensão, pode ser entendido como a manifestação de vontade do indivíduo quanto ao interesse no tratamento, disseminação, processamento e outras ações relacionadas aos seus dados. O prof. Danilo Doneda assim explica:

> O consentimento, nas matérias que envolvem diretamente a personalidade, assume hoje um caráter bastante específico. A evolução tecnológica é responsável por um crescimento das possibilidades de escolha que podem ter reflexos diretos para a personalidade, visto que várias configurações possíveis, referentes tanto à privacidade como à imagem, identidade pessoal, disposições sobre o próprio corpo e outras, dependem em alguma medida de uma manifestação da autonomia privada. O consentimento, ao sintetizar essa atuação da autonomia privada em um determinado momento, há de ser interpretado de forma que seja o instrumento por excelência da manifestação da escolha individual, ao mesmo tempo em que faça referência direta aos valores fundamentais[67].

---

[62]DE SOUSA; DA SILVA, 2020, p. 11.
[63]SARLET, 2022.
[64]SILVA, Lucas Gonçalves; MELO, Bricio Luis da Anunciação; KFOURI, Gustavo. A Lei Geral de Proteção de Dados como instrumento de concretização da autonomia privada em um mundo cada vez mais tecnológico. **Revista Jurídica**, [S.l.], v. 3, n. 56, p. 354 - 377, jul. 2019. ISSN 0103-3506. Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3581/371371972. Acesso em: 23 jul. 2023 doi:http://dx.doi.org/10.26668/revistajur.2316-753X.v3i56.3581. 2019, p. 10.
[65]DE SOUSA; DA SILVA, *op. cit.*, p. 10.
[66]DONEDA, 2020, p. 297.
[67]DONEDA, 2020, p. 297.

Antes de prosseguir, convém perfilhar o conceito de autonomia privada, bem como de autonomia da vontade que com ela se relaciona. Pois bem, pode-se dizer que estes são conceitos fundamentais do Direito, relacionados à liberdade contratual e à capacidade de as pessoas regularem suas relações. A Constituição brasileira estabelece esses princípios por meio dos arts. 1º, IV, e 170, I, que valorizam a livre iniciativa e o trabalho humano, assim como o art. 5º, II, que reforça a liberdade individual[68].

A autonomia da vontade refere-se ao poder de uma pessoa estabelecer negócios jurídicos conforme seus interesses, respeitando os preceitos legais. O Estado deve garantir que as pessoas possam exercer essa autonomia, protegendo-as contra abusos[69]. Já a autonomia privada é vista como o poder reconhecido pelo ordenamento jurídico para que os particulares façam uma autorregulação de seus interesses, produzindo efeitos jurídicos por meio de negócios pactuados[70].

As duas autonomias são próximas, mas distintas: enquanto a autonomia da vontade é uma manifestação subjetiva e psicológica da liberdade individual no campo jurídico[71], a autonomia privada é objetiva, referindo-se ao poder de criar normas específicas dentro dos limites legais. Carlos Alberto Mota Pinto[72] argumenta que ambas representam o mesmo princípio subjacente ao direito privado, enquanto autores como Francisco Amaral[73] diferenciam entre a liberdade de decisão (autonomia da vontade) e o poder de autorregulamentação (autonomia privada).

Segundo Érico de Pina Cabral[74], a autonomia da vontade está ligada à autodeterminação e a autonomia privada ao poder de criar normas próprias. Dessa forma, a autonomia privada é um gênero do qual a autonomia da vontade é uma espécie, focando na liberdade de escolha individual para a criação de obrigações e direitos. Portanto, apesar das

---

[68]BRASIL. **Constituição Federal de 5 de outubro de 1988**. (n.p.)

[69]SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. 2. ed. Rio de Janeiro: Lumen Juris, 2009.

[70]DE MARCO, Cristhian Magnus. **Elementos sobre a autonomia privada e sua relação com o mínimo existencial na teoria dos direitos fundamentais**. In: BAEZ, Narciso Leandro Xavier Baez; CASSEL, Douglas (Orgs.). A realização e a proteção internacional dos Direitos Humanos: desafios do século XXI. Joaçaba: Ed. UNOESC, p. 246-59, 2011, p. 247.

[71]AMARAL, Francisco. **Direito Civil**: introdução. 6.ed. rev. atual. e aum. Rio de Janeiro: Renovar, 2006, p. 345.

[72]PINTO, Carlos Alberto Mota. **Teoria Geral do Direito Civil**. 4.ed. por António Pinto Monteiro e Paulo Mota Pinto. Coimbra: Coimbra Editora, 2005, p. 102.

[73]AMARAL, 2006, p. 345.

[74]CABRAL, Érico de Pina. A "autonomia" no direito privado. In: **Revista de Direito Privado. São Paulo: Revista dos Tribunais**, 19(5)83-129, jul/set 2004, p. 111.

distinções, ambas são essenciais para que os particulares possam exercer sua liberdade e satisfazer suas necessidades dentro dos limites do direito e da justiça social.

No entanto, em que pese a relação estreita com os direitos da livre iniciativa e da liberdade individual, no contexto da proteção de dados pessoais, a autonomia privada não deve ser tratada como um princípio absoluto. Isso ocorre porque a manipulação dos titulares de dados e práticas que os tornam vulneráveis constituem questões graves que afetam diretamente a liberdade de decisão individual. Em determinadas situações, a vontade individual precisa ser relativizada, seja por interferências persuasivas ou manipuladoras que limitam a capacidade de decisão autônoma, seja pelo fato de que certos direitos, sobretudo os de natureza fundamental, não são passíveis de abdicação ou renúncia.

Daniel Sarmento[75] destaca a relevância da autonomia privada e pública como fundamentais para a proteção integral da liberdade humana. Ele argumenta que a liberdade está comprometida quando não são asseguradas as condições materiais mínimas que permitam a vivência plena e consciente dessa liberdade. Isso implica que a simples capacidade de decisão não basta, é necessário que sejam garantidos também os meios materiais e sociais para que essa decisão seja exercida de maneira plena e informada. Dessa forma, a compreensão contemporânea da liberdade vai além da capacidade de escolha, incluindo também a provisão de condições para que essa escolha seja efetiva e significativa.

A ausência de tais condições mínimas, como a superação da pobreza, da fome, do analfabetismo e da exclusão social, impede a plena realização da autonomia, transformando-a em uma liberdade vazia de sentido prático. Diante disso, a autodeterminação informativa e a proteção de dados pessoais devem ser interpretadas levando-se em consideração essas limitações, de modo a garantir não apenas o respeito à autonomia privada, mas também a oferta de condições materiais e sociais que permitam sua realização consciente e eficaz[76]. Assim, a autonomia privada deve ser entendida como um princípio a ser promovido em equilíbrio com outros valores e direitos, buscando uma liberdade efetiva e informada para todos os indivíduos.

A essência do direito fundamental à proteção de dados pessoais é assegurar ao titular a proteção eficiente de seus dados, livrando ele das mazelas a que pode ser acometido em um cenário sem proteção, como à manipulação, controle e até a exclusão desse indivíduo da

[75]SARMENTO, 2009, p. 154.
[76]SARMENTO, 2009, p. 154.

sociedade, em casos mais graves. É fato que a ênfase contemporânea que está sendo dada a este assunto se reflete justamente, como já demonstrado, na valiosidade econômica dos dados e no fato de que possuir as informações dos titulares, em diversos contextos, significa poder. É o caso do mercado digital, que precisa compreender o comportamento do consumidor para estimular a compra, ou dos governos totalitários antigos, como no exemplo alemão citado no início do primeiro tópico, cujos dados pessoais dos cidadãos foram utilizados como instrumento para facilitar a identificação dos judeus e outros grupos perseguidos no contexto do Nazismo.

Por essa razão, é especialmente importante que haja uma tutela protetiva específica sobre os dados pessoais das pessoas e, ainda, que existam travas à sua disposição, tendo em vista os riscos muitas vezes de difícil mensuração por parte do titular. Por essa razão, há a discussão a respeito da propriedade e titularidade atinente aos dados pessoais. Já se avançou na conceituação e compreensão da autodeterminação informativa e da autonomia privada vigente no direito brasileiro. Explicou-se, contudo, que elas não são princípios absolutos, havendo uma necessária relativização, a depender do caso concreto, sobretudo para a eficácia de outros direitos fundamentais.

Bruno Bioni explica que a discussão a respeito da propriedade dos dados não se aplica ao direito pátrio, principalmente pelo fato de que "a negociabilidade dos direitos da personalidade cinge-se à fruição de tais bens (*lato sensu*) e, não, propriamente, à sua titularidade (*stricto sensu*), de acordo com a intelecção dos vocábulos "intransmissibilidade e "irrenunciabilidade" contidos no art. 11 do Código Civil"[77]. Nessa perspectiva, Mendes explica que o questionamento quanto à propriedade dos dados pessoais é uma falsa questão. Na perspectiva da autora, "a natureza do bem protegido, a própria personalidade a que os dados pessoais se referem, exige que a proteção de dados pessoais seja compreendida não como um direito à propriedade, mas como uma espécie de direitos da personalidade"[78]. Tal questão torna-se ainda mais clara com a consagração desse direito como um novo direito fundamental.

Mister tecer considerações ainda quanto à extensão da autodeterminação informacional e seus limites tendo por base o consentimento que, apesar de ser melhor analisado no próximo capítulo, aqui é levantado como parte da discussão sobre a autodeterminação. Em um cenário em que a coleta e o tratamento de dados se tornaram

[77]BIONI, 2021, p. 204.
[78]MENDES, 2014, p. 124.

práticas comuns e abrangentes, é crucial refletir sobre até que ponto o titular desses dados pode dispor deles com base em sua autonomia negocial, conforme apresentado no parágrafo anterior. A regulação desse processo, normalmente guiada por termos de uso e consentimento fornecido pelo titular, não pode se limitar apenas à vontade individual, pois questões maiores, como a proteção da privacidade e do valor social dos dados, precisam ser consideradas[79].

A perspectiva crítica da autodeterminação informativa, centrada unicamente no consentimento, requer uma abordagem mais ampla. Embora a autonomia seja um princípio valioso, ela não deve se tornar uma armadilha que permita práticas prejudiciais ao titular dos dados ou que comprometa a proteção desse território informacional. Em outras palavras, a liberdade de dispor sobre os dados pessoais deve ser acompanhada de mecanismos que preservem sua integridade e finalidade social. Não se trata de negar o consentimento como uma forma válida de autonomia, mas de reconhecer que ele precisa ser complementado por outras normativas que imponham limites e restrições para proteger o indivíduo e a sociedade[80].

A definição de zonas de autonomia requer uma análise cuidadosa dos parâmetros que norteiam o fluxo de informações pessoais. Esse fluxo precisa ser avaliado à luz de sua adequação ao engajamento social e ao desenvolvimento da personalidade do titular dos dados. Uma interferência excessiva pode impactar negativamente na capacidade de o indivíduo exercer seus papéis sociais e desenvolver sua identidade, sendo assim fundamental que a proteção de dados não se torne um obstáculo ao livre desenvolvimento da personalidade[81].

Nesse sentido, a ideia de "privacidade contextual" ganha destaque. Trata-se de investigar como o fluxo de informações pessoais afeta a capacidade dos titulares de cumprir seus papéis sociais e desenvolver suas identidades de maneira autônoma e protegida. Uma análise casuística é necessária para compreender os contextos subjacentes ao tratamento de dados e assegurar que sua integridade seja preservada. Esse enfoque permite identificar práticas que sejam potencialmente disruptivas ao bem comum, evitando fricções sociais indesejadas e promovendo a privacidade informacional como valor central[82].

Portanto, os limites à disposição dos dados pessoais devem ser observados como parte de um direito da personalidade que, embora reconheça a autonomia do titular, impõe

[79]BIONI, 2021, p. 206.
[80]*Ibidem*, p. 206.
[81]BIONI, 2021, p. 206.
[82]*Ibidem*, p. 206.

restrições em consonância com o que determina o art. 11 do Código Civil. Para além disso, deve observar os limites de um direito fundamental. Essa abordagem relativa e contextual da autodeterminação informacional visa equilibrar a autonomia individual com o valor social da proteção de dados, promovendo um ambiente em que a privacidade seja resguardada de forma integral e eficaz. Em suma, a proteção de dados pessoais deve ser entendida como um direito que transcende o consentimento e busca preservar tanto o indivíduo quanto a sociedade em que ele está inserido[83].

1.3. A exploração de dados pessoais na contemporaneidade: análise sobre a vida na sociedade do controle e a função do consentimento

O indivíduo, na era digital, encontra-se em uma posição de dependência do sistema. Isso fica evidente quando a utilização de um site ou ferramenta online está condicionada à aceitação de seus termos de uso[84]. Na realidade pós-moderna, é praticamente inviável manter atividades sociais ou profissionais sem ferramentas digitais, isto é, sem figurar em alguma rede social (instagram, linkedin, facebook, etc.). Assim, a única opção muitas vezes disponível é aceitar os termos de uso para acessar o serviço ou produto desejado. Quando não há opção de recusar a coleta de dados, surge um questionamento sobre a validade do consentimento.

No entanto, essa lógica predominante sobre o consentimento do usuário, especialmente no contexto do consumidor digital, em que frequentemente há uma disparidade de informações, desafia a noção de autodeterminação informativa. A Lei Geral de Proteção de Dados Pessoais, em seu artigo 7°, I, exige o consentimento do titular dos dados para o seu processamento. O artigo 8° da mesma lei garante que este consentimento deve ser "expresso

[83]BIONI, 2021, p. 207.

[84]Os "termos de uso" são contratos de adesão que estabelecem as regras e condições para o uso de um produto, site ou aplicativo, detalhando responsabilidades, condutas esperadas e direitos tanto do prestador de serviços quanto do usuário. Conforme a Lei Nº 12.965/2014, eles incluem normas sobre a utilização da plataforma, proibições, acesso, proteção de propriedade intelectual e limitam a responsabilidade de ambas as partes, ajudando a evitar mal-entendidos e litígios sobre direitos e deveres. Dessa forma, os termos de uso protegem tanto a empresa quanto o usuário, esclarecendo expectativas e responsabilidades na prestação dos serviços (LIRA, Mydyã. **Termos de uso: conheça seus requisitos e sua finalidade**. EJUDI, Ceará: 2023. Disponível em: https://ejudi.com.br/termo-de-uso-finalidade/. Acesso em: 20 set. 2024).

por escrito ou por outro meio que demonstre a vontade do titular". O § 3° ainda afirma que "é proibido o tratamento de dados pessoais baseado em um consentimento viciado"[85].

Dessa forma, a legislação proíbe explicitamente a violação do consentimento do usuário, sendo este um requisito essencial para o tratamento de dados. Qualquer violação dessas normas constitui uma prática abusiva e deve ser sancionada conforme a lei. Contudo, o que se deve questionar é o alcance desse consentimento, visto que frequentemente a recusa em aceitar a política de privacidade ou a coleta de dados impede o acesso ao produto ou serviço desejado, transformando-se em uma barreira que coage o usuário a concordar com as condições impostas pelo controlador para obter acesso. Portanto, a funcionalidade do consentimento pode ser entendida da seguinte maneira:

> Para que o indivíduo possa exercer o seu poder de autodeterminação informativa, faz-se necessário um instituto jurídico por meio do qual se expresse a sua vontade de autorizar ou não o processamento de dados pessoais: o consentimento. Este é o mecanismo que o direito dispõe para fazer valer a autonomia privada do cidadão[86].

Assim, percebe-se que o principal problema em relação ao não consentimento do usuário aos termos de uso de um serviço digital é a potencial exclusão desse indivíduo do mercado de consumo, transformando, em muitos casos, o consentimento em uma mera formalidade[87]. Neste contexto, Rodotà[88] enfatiza a importância de analisar as condições sob as quais o consentimento é dado, para avaliar se ele é baseado em um entendimento adequado e se realmente pode ser considerado como uma escolha livre. Além disso, a proteção do consumidor é essencial, especialmente devido à frequente desigualdade informacional, o que justifica a proteção especial conferida pela legislação consumerista, além da vulnerabilidade inerente ao consumidor.

Rodotà[89] apresenta a noção de "contratante vulnerável", caracterizado pela limitação na liberdade de escolha ao manifestar sua vontade, especialmente em contextos onde o consentimento para o uso de informações pessoais é obrigatório para acessar bens ou serviços essenciais. O autor destaca, ainda, que essa vulnerabilidade se intensifica em situações onde o indivíduo não tem alternativas para obter esses serviços sem ceder seus dados.

---

[85]BRASIL, **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. (n.p.)
[86]MENDES, 2014, p. 60.
[87]*Ibidem*, p. 65.
[88]RODOTÀ, Stefano. **A vida na sociedade da vigilância: A privacidade hoje.** Org. Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.
[89]*Ibidem*.

Ao analisar o sistema de saúde norte-americano, por exemplo, ele observa que o consentimento para a coleta de informações de saúde é essencial para que a pessoa tenha acesso a tratamentos médicos. Em um cenário em que não há um direito fundamental à saúde ou um sistema público de saúde, como ocorre nos Estados Unidos, o modelo privado de seguros prevalece. Nesse sistema, as seguradoras condicionam a celebração de contratos e a cobertura dos custos médicos à entrega de uma quantidade significativa de dados pessoais. Assim, embora a proteção da privacidade seja formalmente reconhecida, na prática, ela se torna um privilégio daqueles que podem arcar diretamente com os custos médicos, sem depender das exigências das seguradoras[90].

Portanto, é apenas em um contexto em que a recusa em consentir com a coleta de dados não resulte em prejuízos desproporcionais para o usuário que se pode realmente considerar a existência de um consentimento autêntico. Caso contrário, sempre que o consentimento for uma exigência para a continuação do uso do serviço, funcionando como uma espécie de moeda de troca, existirá um problema em sua base conceitual. Por outro lado, uma contribuição relevante da legislação, também respaldada academicamente, é o direito à revogação do consentimento. Esse direito pode ser visto como uma manifestação do controle efetivo do titular sobre seus dados.

É que a faculdade de revogar o consentimento a qualquer momento, sem necessidade de justificativas, apresenta mais coerência, considerando a natureza dos dados pessoais como um direito da personalidade e um direito fundamental. A exigência de descumprimento contratual como fundamento para a revogação do consentimento remete a um modelo mais transacional. Contudo, dada a essência dos direitos de personalidade, na qual o exercício do direito à proteção de dados é efetivado através do consentimento, a capacidade de revogação é intrínseca ao próprio direito. Além disso, as dificuldades que o indivíduo enfrenta ao compreender e avaliar as implicações do seu consentimento no início do processo de tratamento de dados justificam a liberdade de revogar o consentimento quando o usuário entender necessário[91].

Conforme estabelecido pelo artigo 8°, § 5°, da LGPD, as pessoas têm o direito de revogar seu consentimento a qualquer momento, mediante uma “declaração explícita do

[90]RODOTÀ, 2008, p. 138.
[91]MENDES, 2014, p. 64-65.

titular, por meio de um processo gratuito e simplificado”[92]. Essa disposição confere ao titular um maior controle sobre seus dados pessoais, permitindo que, caso se sinta desconfortável com o tratamento de seus dados – seja por reconhecer sua vulnerabilidade em determinadas situações ou por não desejar mais que seus dados sejam utilizados –, possa solicitar a remoção de suas informações da base de dados.

Atualmente, os dados pessoais são considerados um recurso valioso na economia da informação[93]. Isso ocorre porque, a partir dos dados coletados sobre o comportamento, preferências e atividades recentes de um indivíduo, torna-se possível recomendar produtos de maneira eficiente. Essa eficácia decorre do fato de que as recomendações geralmente correspondem ao que o usuário está procurando, aumentando as chances de compra. Esse processo é conhecido como publicidade direcionada que, segundo Bioni, consiste

> [...] prática que procura personalizar, ainda que parcialmente, tal comunicação social, correlacionando-a a um determinado fator que incrementa a possibilidade de êxito da indução ao consumo. Essa prática subdivide-se em publicidade (direcionada) contextual, segmentada e comportamental - espécies do gênero publicidade direcionada[94].

A extensão da coleta de dados atingiu um ponto tal que, atualmente, a inteligência artificial consegue avaliar o estado emocional do usuário de um aplicativo. Isso pode ser feito através da análise de *emojis*[95] utilizados em conversas ou mesmo pelo conteúdo textual dessas interações. Além disso, as preferências musicais do usuário em plataformas de *streaming*[96] e outros tipos de conteúdo de entretenimento também fornecem dados valiosos. Essas informações são úteis para os profissionais de marketing, pois permitem a realização do que

---

[92]BRASIL, **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. (n.p.)

[93]BIONI, 2021, p. 6.

[94]*Ibidem*, p. 15.

[95]Os emojis são símbolos gráficos que representam emoções, objetos, ações e ideias, funcionando como uma nova forma de linguagem visual. Muito presentes em chats e redes sociais, eles são usados para complementar ou substituir palavras, facilitando a expressão de sentimentos e intenções de forma rápida e criativa. Por meio dos emojis, as pessoas conseguem transmitir emoções e se identificar de maneira mais lúdica e direta nas conversas digitais (PAIVA, Ana Lorena Nascimento; BISPO, Ronaldo. **Emojis, as emoções representadas graficamente no ciberespaço.** In: Intercom-XIX Congresso de Ciências da Comunicação na Região Nordeste. 2017).

[96]O streaming é uma tecnologia que permite a transmissão de dados via internet em tempo real, sem a necessidade de download prévio para acessar o conteúdo. Dessa forma, é possível assistir a filmes, séries, ouvir músicas ou acessar outros tipos de mídia instantaneamente, sem ocupar espaço de armazenamento no dispositivo e sem a espera para que o arquivo seja baixado. O termo "streaming" vem do inglês, significando "transmissão", e reflete a essência dessa forma de consumo de conteúdo digital, que tornou-se popular pela praticidade e rapidez com que permite o acesso a uma variedade de mídias (XIMENES, Mariana. **O que é streaming?** Hardware.com. 2021. Disponível em: https://www.hardware.com.br/artigos/o-que-e-streaming/. Acesso em: 20 set. 2024).

Bioni[97] denomina de publicidade comportamental. Essa personalização dos anúncios também representa uma forma de vigilância constante das pessoas e, sobre isso, o autor observa que

> É uma realidade, portanto, a estruturação de bases de dados de emoções, a fim de personalizar ainda mais a ação publicitária. Há, por isso, uma vigilância imperativa das pessoas, em especial do potencial consumidor, o que viria desde os seus hábitos de navegação e comportamento na Internet às suas próprias emoções, tornando-o, totalmente transparente. A expressão "consumidor de vidro", cunhada por Susanne Lace, alcança seu êxtase[98].

O desenvolvimento tecnológico e a incorporação da inteligência artificial no cotidiano têm aumentado a dependência das pessoas em relação a dispositivos tecnológicos e digitais. Por um lado, isso traz a promessa de simplificação de tarefas complicadas e demoradas, como a gestão de agendas. Por outro, existe o ônus relacionado ao compartilhamento de dados pessoais. Esta coleta abrange desde o histórico de pesquisas na internet até informações sobre locais visitados, interações sociais, preferências de conteúdo, curtidas, tempo gasto em diferentes redes sociais e padrões de uso ao longo do dia. A inteligência artificial reúne e analisa esses vastos conjuntos de dados (*big data*) para influenciar o comportamento dos usuários.

A atenção dos usuários se tornou um ativo valioso no contexto do mercado digital, cujo passo inicial do processo de vendas é a atração da atenção do consumidor[99]. Uma das principais formas de medir o engajamento dos indivíduos nas redes sociais é o tempo que eles passam nelas. Isso torna os usuários mais atrativos para empresas que promovem seus produtos online através de marketing[100]. Para garantir o interesse contínuo dos usuários, os desenvolvedores elaboram estratégias para mantê-los engajados, desde notificações de publicações na tela de bloqueio até alertas de novas mensagens ou atualizações nas redes sociais. Tudo é cuidadosamente planejado para incentivar o uso constante e a permanência nesses ambientes virtuais. Nesse contexto, a literatura é categórica ao afirmar que,

> De posse da enorme quantidade de dados pessoais recolhidos pela inteligência artificial e processadas por Big Data, os profissionais de marketing e os

[97] BIONI, 2021.

[98] *Ibidem*, p. 22.

[99] SOUZA, Joyce; AVELINO, Rodolfo; DA SILVEIRA, Sérgio Amadeu. **A Sociedade de Controle: Manipulação e modulação nas redes sociais**. Hedra: São Paulo, 2018, p. 25.

[100] O marketing é uma função organizacional e um conjunto de processos voltados para a criação, comunicação e entrega de valor ao cliente, bem como para a gestão de relacionamentos que beneficiem a empresa e seus stakeholders. Segundo a definição de 2004 da American Marketing Association (AMA), o marketing vai além da simples promoção de produtos e envolve todas as áreas da organização, focando na satisfação do cliente e na construção de confiança e comprometimento para manter relacionamentos duradouros. A nova abordagem do marketing reconhece a importância dos stakeholders, garantindo que a relação entre empresa e consumidor não prejudique a sociedade como um todo. Assim, o marketing moderno busca não apenas criar valor para os clientes, mas também atuar de forma ética e responsável, promovendo o bem-estar da sociedade (FREDERICO, Elias. **O que é Marketing**. Antenna Web, v. 4, n. 1, 2008, p. 3).

> desenvolvedores de softwares têm um colosso de oportunidades jamais visto para criar mundos e vender oceanos azuis, ampliando os lucros de suas empresas[101].

A discussão quanto ao *design* e *layout* será aprofundada em páginas vindouras neste estudo, no entanto, aqui cabe mencionar, em linha com o que se argumentou acima sobre as estratégias utilizadas pelo mercado para prender a atenção do usuário, sobre o design viciante. Esse termo tem sido amplamente utilizado em discussões no âmbito da União Europeia e se refere às estratégias de design de sites, aplicativos e redes sociais que são utilizados com o objetivo de prender a atenção do usuário pelo maior período possível.

Nesse contexto, o Parlamento Europeu aprovou a Resolução de 12 de dezembro de 2023, denominada "*on addictive design of online service and consumer protection in the EU single market*" (2023/2043(INI)). Esse normativo cria normas com vistas à mitigação dos casos de dependência das redes sociais, intervindo no layout desses instrumentos. Como explica Sofia Fernandes[102], enquadra-se no conceito de "design viciante" elementos como a rolagem infinita da tela, vídeos com automatização da reprodução, sequência de sugestão de conteúdos ao término dos vídeos e outros elementos que são capazes de manipular o autocontrole das pessoas.

A resolução em questão reflete sobre o modelo de negócios baseado na atenção de certas empresas de tecnologia, que exploram vulnerabilidades dos usuários para prolongar o tempo gasto em suas plataformas. Esse modelo se aplica principalmente a serviços que monetizam dados ou mantêm usuários engajados para coleta de informações, incluindo redes sociais, jogos online, serviços de *streaming* e *marketplaces*[103].

Os considerandos ressaltam que o "design viciante" ou "design manipulativo" tem impactos significativos sobre o comportamento dos consumidores, criando formas de dependência digital que afetam negativamente a saúde física e mental, especialmente de crianças e adolescentes. Há uma distinção entre modelos de negócios, com alguns serviços dependendo da monetização de dados e outros operando por assinaturas, e nem todos apresentam características viciantes. No entanto, mesmo quando tais características não estão

---

[101]SOUZA; AVELINO; DA SILVEIRA, 2018, p. 26.

[102]FERNANDES, Sofia. O que é design viciante e por que a UE quer limitar seu uso? **Deutsche Welle**. Direitos Humanos - Alemanha. Publicado em 12/06/2024. Disponível em: https://p.dw.com/p/4gwbI. Acesso em: 15 set. 2024.

[103]EUROPEAN PARLIAMENT. **Resolução do Parlamento Europeu de 12 de dezembro de 2023 sobre o design viciante de serviços em linha e a proteção do consumidor no mercado único da UE (2023/2043(INI))**. 2023. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.html. Acesso em: 15 set. 2024.

presentes, é destacada a importância de que o desenvolvimento de aplicativos e serviços seja feito de maneira ética e responsável[104].

O considerando B aponta os efeitos positivos dos serviços digitais, como a eficiência, a conectividade e a acessibilidade, mas ressalta que esses avanços trazem também desafios, exigindo atenção política para questões de saúde física e mental. Os jovens, por exemplo, passam em média mais de sete horas diárias online (considerando C) e há uma relação comprovada entre o uso excessivo de smartphones e o desenvolvimento de problemas de saúde mental, incluindo depressão e ansiedade, além de impactos negativos sobre o desempenho escolar e o desenvolvimento psicossocial[105].

Outro ponto importante é a relação entre o uso excessivo da Internet e a saúde pública, comparando seus efeitos aos de dependências relacionadas a substâncias (considerando D). Destaca-se a necessidade de uma regulamentação rigorosa para prevenir a dependência digital e proteger os consumidores, especialmente crianças e jovens que são mais vulneráveis. O design viciante pode comprometer a concentração, estimular pressões sociais para estar constantemente conectado e levar a uma sobrecarga de informações (considerando G), e essas práticas podem ter impactos diferenciados de acordo com o gênero e faixa etária dos usuários (considerando H)[106].

Os considerandos I e J focam na maneira como os designs viciantes exploram vulnerabilidades psicológicas e emocionais, utilizando técnicas de gamificação, recompensas variáveis e mecanismos de interação social (como notificações push e curtidas) para manter os usuários engajados. Essas práticas podem levar a comportamentos compulsivos e ao aumento de padrões comportamentais de uso excessivo, prejudiciais sobretudo a crianças que ainda estão em fases críticas de desenvolvimento[107].

Há também preocupações com o desequilíbrio de poder e a assimetria digital causada por sistemas baseados em dados (considerando K), em que os consumidores são constantemente confrontados com inteligências artificiais que exploram suas vulnerabilidades. O design viciante é frequentemente associado a elementos persuasivos

---

[104] *Ibidem*.

[105] EUROPEAN PARLIAMENT. **Resolução do Parlamento Europeu de 12 de dezembro de 2023 sobre o design viciante de serviços em linha e a proteção do consumidor no mercado único da UE (2023/2043(INI))**. 2023.

[106] *Ibidem*.

[107] *Ibidem*.

como rolagem infinita, reprodução automática e notificações, que afetam diretamente o comportamento do usuário (considerando L)[108].

Em termos regulatórios, a Lei dos Serviços Digitais da UE (LSD) introduziu obrigações de transparência e proibições de padrões obscuros em sistemas de recomendação, mas há críticas sobre a abrangência das disposições existentes, que não cobrem todos os serviços problemáticos, como jogos online (considerandos M e P). Além disso, a legislação futura sobre inteligência artificial visa proibir sistemas de IA manipuladores, mas apenas na medida em que utilizam técnicas enganosas deliberadamente[109].

Finalmente, o considerando O aborda os desafios de simplesmente impor limites de tempo ao uso de serviços online, destacando que essas medidas transferem a responsabilidade para o indivíduo, ao invés de abordar as questões estruturais do design viciante. Há também uma discussão sobre a importância de medidas de segurança desde a concepção, controles parentais e alfabetização digital como formas de mitigar os riscos para crianças e adolescentes[110].

A resolução, portanto, reflete a necessidade de uma abordagem equilibrada, que promova tanto os benefícios dos serviços digitais quanto a proteção dos consumidores contra práticas de design manipulativo e viciante, com especial atenção para a saúde física e mental de crianças e adolescentes e a transparência das plataformas digitais, temas de grande repercussão e de suma relevância no contexto da proteção de dados pessoais, posto que com ela se interligam.

Além do desenvolvimento de estratégias de design viciantes, as *big techs* desenvolveram mecanismos de customização dos aplicativos a partir das preferências do usuário, que são obtidas pelo histórico de buscas, acessos mais frequentes e pela própria perfilização em si. Ou seja, o usuário encontra no ambiente digital “o melhor dos mundos”, ficando preso ou viciado na utilização daquela interface, pela hiperestimulação e satisfação que recebe ao estar diante de todo esse conjunto arquitetado para prender-lhe a atenção.

É indiscutível que, no atual contexto social, as mídias sociais e diversos websites na internet funcionam como influenciadores de opinião. Isso não ocorre por acaso. A sociedade

---

[108]*Ibidem*.

[109]EUROPEAN PARLIAMENT. **Resolução do Parlamento Europeu de 12 de dezembro de 2023 sobre o design viciante de serviços em linha e a proteção do consumidor no mercado único da UE (2023/2043(INI))**. 2023.

[110]*Ibidem*.

moderna adotou o conceito de “mundo virtual”, que existe paralelamente à realidade tangível. Neste universo digital, que envolve as mesmas pessoas do “mundo real”, o controle é mais facilmente exercido, visto que o dispositivo de controle está, frequentemente, nas mãos dos próprios usuários, de forma voluntária.

Nesse cenário, torna-se viável influenciar o comportamento dos consumidores para assegurar o êxito nas vendas. Pode-se afirmar que o marketing tem um papel direto na influência do comportamento do consumidor, chegando a moldá-lo. A respeito disso:

> Mas, pergunta Lazzaroto (2006, p. 103), como o marketing pode produzir a mudança na sensibilidade do consumidor e estimulá-lo a comprar? Que tipo de subjetivação é mobilizada pela publicidade? Para ele, o turbilhão de encadeamento de imagens e sons cria uma nova sensibilidade em quem assiste àquele conteúdo. Revela um mundo possível que existe, mesmo que exista somente no universo da própria propaganda. Referem-se aos signos de mundos possíveis, gerando desejos de pertencimento a esses mundos (assim como frustrações por não conseguir integrá-los - e impedir que outras multiplicidades concorrentes se constituam - é quando a sociedade de controle assume a forma de expropriação capitalista contemporânea (2006, p. 1780)[111].

Portanto, todos esses mecanismos juntos formam o que pode ser denominado de "sociedade do controle", na qual é possível influenciar os desejos mais profundos dos indivíduos, incitando-os constantemente ao consumo. Contudo, consideram-se como abusivas, segundo o Código de Defesa do Consumidor (art. 37, §2°), práticas como publicidade discriminatória, que incite à violência, explore medo ou superstição, se aproveite da inexperiência das crianças, desrespeite valores ambientais ou induza comportamentos prejudiciais à saúde ou segurança do consumidor. Conforme Tartuce e Neves[112], essa lista é exemplificativa, não exaustiva. Assim, existem outras formas de publicidade abusiva, especialmente aquelas que incentivam o consumismo e podem levar ao superendividamento, cuja prevenção é uma obrigação social.

Na pós-modernidade, o consumo está vinculado à satisfação pessoal, há uma associação da felicidade ao ato de consumir, possuir e exibir produtos. Neste cenário, grandes marcas, utilizando estratégias persuasivas, conquistaram o controle psíquico-emocional dos consumidores na era digital. O consumo de bens e serviços desnecessários tem substituído as necessidades básicas em muitos casos e isso pode ser evidenciado pelo comportamento de consumidores que se endividam para adquirir novos produtos, acreditando na essencialidade destes, prejudicando suas finanças pessoais.

---

[111]SOUZA; AVELINO; DA SILVEIRA, 2018, p. 19-20.

[112]TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. **Manual de direito do consumidor**: direito material e processual. rev. e atual. Rio de Janeiro: Método, 2017, p. 457.

As grandes marcas, por meio de mensagens subliminares, persuadem os consumidores da indispensabilidade de seus produtos, indo além da mera convicção e criando uma cultura de consumo. Assim, ocorre o que pode ser considerado um assédio ao consumo, situação em que a suposta persuasão é, de fato, uma "intromissão não autorizada no subconsciente do indivíduo com potencial para interferir na sua autonomia e escolhas"[113].

As estratégias da indústria publicitária promovem um deslocamento do consumo racional para o consumo emocional, influenciando a percepção dos consumidores sobre suas necessidades e desejos. Com isso, há uma tendência de confundir necessidades reais com aquelas artificialmente criadas pelo mercado, resultando em um desejo que aparenta ser uma necessidade atendida apenas por um produto específico. A literatura sobre o tema destaca que o principal objetivo da publicidade é incentivar o consumo por meio de táticas que exploram tanto necessidades humanas reais quanto aquelas artificiais. Quando a publicidade atua no nível inconsciente e gera reações emocionais que determinam as escolhas de consumo, mascarando sua finalidade comercial, ocorre o que os autores definem como "assédio subliminar ao consumo"[114].

Além disso, é relevante abordar o conceito de *storytelling*, uma estratégia publicitária que busca dar um novo significado ao produto, incorporando-o em um contexto emocional. Essa técnica visa atribuir ao produto qualidades que despertam emoções e conexões, tornando-o mais atraente e envolvente, fazendo com que o consumidor se visualize utilizando-o. As grandes marcas utilizam uma variedade de temas em suas narrativas, desde o empoderamento feminino até a luta contra padrões estéticos convencionais e questões de desigualdade social.

O uso de estratégias emocionais pelas marcas é uma forma eficaz de estabelecer uma conexão entre o consumidor e o produto. Esse vínculo emocional pode levar a uma identificação pessoal com o produto, ao ponto de o consumidor ser persuadido a acreditar na necessidade de adquiri-lo. Essa técnica atua no subconsciente do consumidor, gerando uma sensação de pertencimento e identificação que vai além das características funcionais do

[113]VERBICARO, Dennis; RODRIGUES, Lays; ATAÍDE, Camile; Desvendando a vulnerabilidade comportamental do consumidor: uma análise jurídico-psicológica do assédio de consumo. **Revista de Direito do Consumidor**, 119. 349-384, São Paulo, 2018. p. 365.
[114]VERBICARO, Dennis; RODRIGUES, Lays; ATAÍDE, 2018, p. 14.

produto. Dessa forma, o engajamento é construído não só em torno da utilidade, mas também das emoções e valores associados ao bem ou serviço promovido[115].

Como dito acima, a partir da utilização de técnicas como o *storytelling*, as marcas buscam humanizar seus produtos, construindo uma narrativa que permita aos consumidores se identificarem com a história e os valores apresentados. Conforme argumentam Verbicaro, Rodrigues e Ataíde[116], essas histórias facilitam o estabelecimento de um diálogo real entre a marca e o consumidor, transcendendo barreiras como classe econômica, faixa etária ou gênero. Através desse processo, os vínculos criados entre consumidor e marca se tornam mais profundos e duradouros, pois o consumidor passa a ver no produto não apenas um bem material, mas um reflexo de suas próprias experiências, emoções e valores.

A transformação do consumo em uma ferramenta de satisfação pessoal, centrada na exploração dos aspectos emocionais do indivíduo, destaca um desafio significativo na era pós-moderna. Nesse contexto, a lógica consumista intensifica o apelo às emoções, levando os consumidores a buscarem produtos e serviços que não só atendam às suas necessidades práticas, mas também satisfaçam desejos induzidos pelo mercado. Isso reforça a importância de proteger os consumidores contra práticas de assédio de consumo, que exploram essas vulnerabilidades emocionais para impulsionar o consumo e moldar percepções de necessidade e desejo.

A literatura ressalta que essa necessidade de proteção cresce à medida que a lógica consumista se torna predominante, colocando os consumidores em uma posição de constante pressão e exposição ao assédio. Como apontam Verbicaro, Rodrigues e Ataíde[117], as necessidades dos consumidores deixam de ser apenas utilitárias e passam a ser impostas pela indústria cultural de massa, gerando um estado de consumo compulsório. Tal imposição afeta não só a liberdade de escolha, mas também a identidade social dos consumidores, uma vez que o não atendimento dessas demandas pode levar à estigmatização social. Assim, a proteção ao consumidor deve ser um valor fundamental e orientador na sociedade atual, contrapondo-se à pressão da lógica consumista.

Com o acesso a uma vasta quantidade de dados, as empresas, utilizando algoritmos avançados, facilmente manipulam o comportamento dos usuários para definir tendências de consumo. Essa influência se torna ainda mais eficaz devido à publicidade personalizada, que

---

[115] *Ibidem*, p. 17.
[116] *Ibidem*, p. 17.
[117] VERBICARO, Dennis; RODRIGUES, Lays; ATAÍDE, 2018, p. 7.

oferece produtos que se alinham perfeitamente com as preferências do indivíduo, através de anúncios repetidos até que a compra seja realizada. Além disso, compreender os interesses específicos de um segmento de mercado é extremamente benéfico para os fornecedores, que podem explorar esses pontos durante a venda, utilizando estratégias de *storytelling*, como visto.

As redes sociais são aliadas valiosas das grandes marcas, pois é através dos dados gerados nelas que se identificam as preferências detalhadas dos indivíduos. Até mesmo uma simples curtida em um conteúdo pode revelar muito sobre as inclinações de uma pessoa. Assim, um conjunto de informações, como histórico de buscas, contatos, locais visitados e conteúdos consumidos, traça o perfil de consumo do usuário. A posse desses dados é extremamente lucrativa, pois além de personalizar a publicidade, as empresas podem praticamente garantir a efetivação da venda. Com tantas ferramentas de influência em um ambiente de controle, a probabilidade de sucesso na venda é muito alta.

Nesse contexto, surge a preocupação com a violação da liberdade de escolha do consumidor, que pode ser classificada como uma prática abusiva e uma forma de publicidade invasiva, conforme o art. 37, § 2°, do Código de Defesa do Consumidor.

Através de um processo automatizado conhecido como perfilização, os controladores de dados conseguem categorizar e individualizar os titulares de dados para facilitar o tratamento dessas informações[118]. Contudo, muitas vezes, os métodos utilizados para essa categorização não são transparentes e a separação dos dados pode ser obscura, conforme apontado por Marques e Mucelin[119]. Embora o GDPR trate especificamente deste tema, a LGPD brasileira não o aborda diretamente. No entanto, a legislação nacional estabelece que dados anonimizados, quando usados para criar um perfil comportamental de uma pessoa identificável, são equivalentes a dados pessoais[120].

Atualmente, não há na legislação brasileira uma definição específica para decisão automatizada, mas, segundo Marques e Mucelin[121], o Projeto de Lei n° 4.496/2019 pode vir a solucionar esse vácuo ao propor a inclusão deste conceito na LGPD. Com isso, poderiam

---

[118]MARQUES, Cláudia Lima; MUCELIN, Guilherme Antônio B. **Inteligência artificial e "opacidade" no consumo**: a necessária revalorização da transparência para a proteção do consumidor. In: O direito civil na era da inteligência artificial. São Paulo: Thomson Reuters Brasil, 2020, p. 413.

[119]*Ibidem*, p. 414.

[120]*Ibidem*, p. 415.

[121]*Ibidem*, p. 416.

ser estabelecidos critérios para a tomada de decisões automatizadas, garantindo maior segurança e conformidade com os direitos individuais.

Os controladores de dados têm acesso a uma ampla gama de informações sobre indivíduos, desde a localização geográfica até características físicas, e esses dados podem ser utilizados de maneira discriminatória. Marques e Mucelin[122] detalham em seu estudo casos de racismo praticados por empresas que, ao usar esses dados, privilegiavam pessoas brancas em detrimento das negras no acesso a serviços. Além disso, os autores relatam situações em que empresas cobram preços diferentes com base no local de residência dos clientes ou oferecem condições de crédito mais favoráveis para homens do que para mulheres, mesmo com condições financeiras semelhantes.

A partir dessas observações, fica evidente que os controladores de dados muitas vezes realizam processamentos que discriminam os consumidores, tendo em mãos seus dados pessoais. Como Marques e Mucelin[123] ressaltam, tais práticas são claramente proibidas pela Constituição Federal (art. 3°, IV), pelo Código de Defesa do Consumidor (arts. 37, § 2°, e 39, IV) e pela LGPD (art. 5°, II). Esta última lei classifica informações acerca da "origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou organizacional, saúde, vida sexual, dados genéticos ou biométricos", como dados sensíveis que, por seu potencial discriminatório, são especialmente protegidos[124].

Outro problema grave relacionado ao mau uso de dados pessoais é a possibilidade de excluir consumidores do mercado. Isso acontece, por exemplo, quando um *score* de crédito baixo resulta na negação de acesso a bens e serviços ou à oferta de condições de compra menos favoráveis. Sobre essa exclusão, a LGPD estabelece no art. 21 que "os dados pessoais relacionados ao exercício regular de direitos pelo titular não podem ser usados em seu detrimento"[125], apontando assim uma hipótese de violação à própria LGPD e aos direitos dos consumidores.

A transparência, enquanto princípio associado ao dever de informação e como parte integrante da boa-fé objetiva, deveria orientar as práticas comerciais de forma a garantir clareza e equilíbrio nas relações de consumo. Contudo, sua efetiva implementação tem se

---

[122] *Ibidem*, p. 418.
[123] MARQUES; MUCELIN, 2020, p. 419.
[124] *Ibidem*, p. 419.
[125] BRASIL, **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. (n.p.)

mostrado insuficiente nos contextos atuais, especialmente com a crescente adoção de tecnologias de inteligência artificial (IA). Embora a transparência seja mais facilmente observada em relação aos bens de consumo, ela se torna problemática quando aplicada às práticas comerciais que utilizam IA, uma vez que tais tecnologias introduzem complexidades significativas na comunicação e no processamento de dados envolvidos nas transações.

Marques e Mucelin[126] destacam que o funcionamento dessas tecnologias de IA frequentemente é referido como "black boxes" (caixas-pretas), devido à dificuldade de compreender e auditar como esses sistemas processam dados e fornecem resultados. Esse termo reflete a falta de transparência inerente às práticas comerciais que empregam IA, uma vez que a forma como essas tecnologias tomam decisões ou fornecem feedbacks é muitas vezes opaca tanto para os consumidores quanto para as empresas. Tal cenário evidencia um desequilíbrio na relação de consumo e destaca a necessidade de regulamentação e de mecanismos que assegurem uma transparência mais efetiva e acessível aos consumidores.

Logo, a transparência é um princípio incorporado ao Código de Defesa do Consumidor, particularmente na Política Nacional das Relações de Consumo (art. 4°, caput, do CDC). Segundo a literatura, ela é vista como "uma regra orientadora fundamental para todo o mercado de consumo e para o sistema de defesa do consumidor"[127]. Como tal, é um pilar essencial para assegurar o equilíbrio nas relações de consumo, atuando como um mecanismo eficaz para reduzir a vulnerabilidade informacional do consumidor.

Embora a transparência nas relações de consumo seja um princípio de ordem pública e de interesse social, sua efetividade depende da integração com outros instrumentos legais. A transparência, associada à boa-fé objetiva, serve como base deontológica para o dever de lealdade e cooperação nas práticas comerciais, promovendo confiança e equilíbrio entre as partes envolvidas. No entanto, para que a transparência não se reduza a um simples argumento teórico, ela precisa ser acompanhada por mecanismos legais que garantam seu cumprimento e eficácia nas relações de consumo.

Além disso, a transparência é entendida como uma via de mão dupla, ou seja, deve ser praticada por ambos os sujeitos envolvidos na relação de consumo: consumidores e fornecedores. Entretanto, ela é atribuída com maior intensidade aos fornecedores, devido ao desequilíbrio informacional e técnico presente nos ambientes virtuais, que acentua a

[126]MARQUES; MUCELIN, 2020.
[127]MARQUES; MUCELIN, 2020, p. 422.

vulnerabilidade dos consumidores. Marques e Mucelin[128] argumentam que essa vulnerabilidade, conhecida como "vulnerabilidade virtual", reforça a necessidade de os fornecedores garantirem clareza e acessibilidade das informações, assegurando que os consumidores possam tomar decisões informadas e conscientes.

Portanto, a transparência é um aspecto crucial que deve ser mantido pelos controladores de dados como um princípio orientador e um dever na condução de qualquer tratamento de dados pessoais. Para alcançar isso, é fundamental criar protocolos de conformidade que sejam integrados nas práticas de governança corporativa. Além disso, a legislação que regula a proteção de dados deve dar ênfase ao princípio da transparência, seja através de políticas públicas que incentivem boas práticas ou por meio de regulamentação específica, dada a sensibilidade e a relevância do tema para assegurar o bem-estar geral.

Para equilibrar a transparência com a tomada de decisão automatizada, Marques e Mucelin[129] sugerem a implementação de um “direito à explicação”. Esse direito garantiria que os titulares dos dados compreendam em detalhes como seus dados são processados, incluindo não apenas a finalidade e o destino dos dados, mas também o procedimento em si. Os autores notam que já existe um direito semelhante no contexto do histórico de crédito, estabelecido através da interação entre o Código de Defesa do Consumidor, a Lei do Cadastro Positivo e interpretações do STJ[130].

[128] *Ibidem*.
[129] MARQUES; MUCELIN, 2020, p. 415.
[130] *Ibidem*, p. 416.

2 O DIREITO DO CONSUMIDOR À PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DO COMÉRCIO ELETRÔNICO E A OBTENÇÃO DO CONSENTIMENTO VÁLIDO

2.1 Comércio Eletrônico e Direito do consumidor: a vulnerabilidade do consumidor no ambiente digital

2.1.1 *Evolução das práticas de consumo*

Pode-se dizer que após a Segunda Guerra Mundial, com a respectiva modernização da indústria, pontuada pela "passagem do modelo de desenvolvimento industrial para o informacional/digital"[131], tem-se uma modificação concreta dos padrões de consumo. Isso pode ser visto principalmente na intensificação das práticas de consumo, marcadas também pela produção de bens em massa, que encontram como grande incentivador a mídia. Esse esforço, inicialmente, se deu com vistas a aumentar o consumo das pessoas e, como consequência, influenciar nas vendas e na geração de emprego e renda[132].

Nesse contexto, a industrialização e a produção em larga escala de produtos padronizados contribuíram para a construção de uma cultura de massas, inclusive no âmbito das artes, como na música e cinema, sendo inserida nesse contexto a ideia de que o bem-estar poderia ser conquistado através do consumo[133].

No cenário de intensificação das relações de consumo, notou-se um avanço na esfera dos direitos fundamentais, de onde surge o direito do consumidor. Nesse compasso, teve o seu amplo reconhecimento em 1973 pela ONU, como direitos fundamental e universal. Após isso, por meio da Resolução nº 39/248 de 1985, também da ONU, houve um incentivo para que os países abordassem e regulamentassem internamente o assunto, o que teve importante reflexo na Constituição Federal de 1988 no Brasil e na feitura do Código de Defesa do Consumidor em 1990[134].

---

[131]MAGALHÃES NETO, F. B. de .; MAGALHÃES, L. B. B. de . A evolução do direito do consumidor e o comércio eletrônico: abordagem pelo direito internacional. **Revista de Direito da ADVOCEF**, [S. l.], v. 13, n. 25, p. 123–142, 2017. Disponível em: https://revista.advocef.org.br/index.php/ra/article/view/318. Acesso em: 05 mai. 2024. 2017, p. 126.

[132]*Ibidem*, p. 126.

[133]ADORNO, Theodor. **Dialética do esclarecimento**. Editora Schwarcz-Companhia das Letras, 1985.

[134]MAGALHÃES NETO; MAGALHÃES, *op. cit.*, p. 126.

A forma como se consolidou o estatuto protetivo consumerista mostra que a sociedade já reconhecia naquele contexto os conceitos de vulnerabilidade e hipossuficiência. Nota-se que, apesar de ter sido feito uma década antes dos anos 2000, o Código de Defesa do Consumidor, por ser uma norma principiológica, conseguiu e ainda consegue, em grande medida, abarcar as mais corriqueiras situações que se integram no dia a dia do consumo.

A modernização da economia, com a inserção de práticas digitais, a ascensão da internet e o universo das compras on-line, fruto também da globalização, facilitou a vida cotidiana das pessoas, reduziu espaços e em muitos casos liberou fronteiras. No entanto, visto por outra ótica, a criação de uma cultura virtual agravou uma série de problemas que já existiam, como a questão do consumismo ou do consumo de massas, bem como permitiu a existência de novos problemas, como a superexposição das pessoas no ambiente on-line.

O final do século XX foi marcado por grandes transformações na estrutura social a nível mundial, conforme explica Lévy[135], sendo que houve naquele contexto diversos grandes eventos que permitiram atravessar "uma fronteira de planetarização notável". O autor cita exemplos dessa grande transformação, como a finalização da bipolaridade na esfera política a nível global, o boom do ciberespaço, a corrida pela globalização da economia, o desenvolvimento do comércio a nível internacional, entre outros acontecimentos.

Assim, pode-se dizer que o comércio eletrônico surge, nesse contexto, como uma importante atividade, que funciona inclusive como meio para a consolidação dessa economia digital[136]. Magalhães Neto e Magalhães destacam, ainda, que

> A atividade mais incentivada nessa nova era de comunicação é o comércio eletrônico, realizado por meios tecnológicos como a internet, principalmente o comércio eletrônico entre consumidor e produtor/fabricante.
>
> Tal comércio possibilita que ofertas, informações e produtos estejam disponíveis em qualquer lugar instantaneamente 24 horas por dia, durante todos os dias do ano, sem necessidade nem mesmo de uma loja física[137].

Esse novo modelo econômico, que aqui será chamado de economia digital, possui como maior ativo a informação das pessoas e sobre as pessoas. É fato que esse novo modelo econômico e todas as práticas de que se utiliza, que já foram mencionadas no âmbito desse estudo como os *retargetings*, os *cookies*, dentre outros, serviram para agravar a vulnerabilidade do consumidor no ambiente virtual, ao passo que a sua escolha se torna

---

[135]LÉVY, Pierre. **A conexão planetária**. O mercado, o ciberespaço, a consciência. 1ª reimpressão. Tradução de Maria Lucia Homem e Ronaldo Entler. São Paulo: Ed. 34, 2003, p. 24.

[136]MAGALHÃES NETO; MAGALHÃES, 2017, p. 127.

[137]*Ibidem*, p. 127.

paradigmática, senão inviável, pois a escolha até pode acontecer entre um produto e outro, mas terá como resultado fatídico o consumo, haja vista que o sistema é programado para isso.

Campos explica que a ordem social, que antes estava baseada nas organizações, enfrentou uma grande transformação com o surgimento dos novos instrumentos eletrônicos de comunicação. Para o autor, "a nova ordem digital, que reestruturou a antiga ordem das organizações baseadas no conhecimento, é caracterizada em particular pela inteligência artificial, *big data* e algoritmização, e tem produzido as formas e o *design* da nova ordem do conhecimento no contexto da digitalização"[138].

Todas essas transformações ocasionam uma alternância da realidade com a virtualidade, misturando-se às concepções de concreto e real as noções de abstrato e fantasioso. É fato que o pseudo mundo criado no ambiente virtual, mormente nas redes sociais, por meio das quais as pessoas estão erigindo impérios patrimoniais e onde se dizem autoridades em diversos assuntos sem necessariamente possuírem precedentes de formação ou a construção de uma carreira que lhe torne apta a opinar, estão transvalorando os valores sociais e alterando até mesmo a lógica da verdade, naquilo que se convencionou chamar de pós-verdade.

Ainda sobre a forma como as plataformas influenciam a dinâmica da sociedade e da vida humana, alterando a forma como os indivíduos vivem, Campos diz que elas

> [...] geram uma nova base artificial para a vida humana ou uma nova plataforma para o projeto da vida humana e o livre desenvolvimento da personalidade. O digital transforma não apenas a geração de conhecimento social, mas também as interações e experiências mais íntimas de indivíduos uns com os outros e com as instituições, que influenciam de forma decisiva suas trajetórias sociais[139].

Observa-se, logo, que a vida se desenvolve em um novo ciclo de existências, em que se inserem a existência virtual do ser humano e a formação de novos grupos sociais, como os denominados *influencers* atualmente. O que se altera com essa dinâmica é não apenas as estruturas sociais, mas o comércio e a forma como as relações de consumo se dão.

Nesse contexto, para fazer jus à modernização, surge o comércio eletrônico e demais práticas a ele correlatas, cuja ascensão levou à irradiação dos desafios da esfera do direito do

---

[138]CAMPOS, Ricardo. **Metamorfoses do direito global**: sobre a interação entre direito, tempo e tecnologia. São Paulo, SP: Editora Contracorrente, 2022, p. 256.
[139]*Ibidem*, p. 257.

consumidor para muitas outras, como para o direito penal, direito internacional, direito comercial e do direito civil, sem prejuízo de outras áreas[140].

Diante das muitas mudanças observadas na forma de contratar no ambiente virtual em relação à realidade física, há também a modificação da forma como é visto o próprio contrato. Assim, para além da forma do contrato (físico x digital), há preocupações com relação à sua lisura, como explicam Magalhães Neto e Magalhães:

> A diferença entre um contrato tradicional e um contrato eletrônico está em sua forma, como também a problemática da manutenção de sua integridade, livre de adulterações, e a questão da assinatura digital, visando a prevenção de fraudes, cujas ocorrências multiplicam-se, inclusive com apropriação indevida de dados, compras e saques em contas de terceiros através de invasões de hackers. Busca-se segurança e confiabilidade, como também a integridade da mensagem, a segurança da informação e a proteção dos dados pessoais no meio eletrônico, tendo em vista que a vulnerabilidade do consumidor agrava-se no ambiente virtual[141].

Nota-se que o amparo ao consumidor se torna mais difícil no ambiente virtual, haja vista que, para além das grandes burocracias enfrentadas para conseguir atendimento humano, em muitos casos pela ausência de um SAC que seja efetivo, há dificuldades também relacionadas à operacionalidade da logística de entrega dos produtos e serviços contratados, com atrasos injustificados, erros de endereço e até mesmo dos produtos, entre uma série de outras dificuldades que excedem a seara do mero aborrecimento.

Por essa razão, há uma constante fiscalização dos órgãos de proteção e defesa do consumidor, com vistas a assegurar o cumprimento de requisitos mínimos para a melhor experiência do consumidor em suas compras on-line.

2.1.2 *A vulnerabilidade no âmbito do comércio eletrônico*

A vulnerabilidade do consumidor é reconhecida como um princípio no âmbito da Política Nacional das Relações de Consumo, estabelecida pelo art. 4º do Código de Defesa do Consumidor[142]. Assim, o reconhecimento da vulnerabilidade do consumidor, além de um princípio a ser reconhecido no âmbito do mercado de consumo (art. 4º, I), é uma premissa para o tratamento dele em todas as relações estabelecidas com o fornecedor, sendo também

[140]MAGALHÃES NETO; MAGALHÃES, 2017, p. 127.
[141]*Ibidem*, p. 128.
[142]BRASIL. **Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 20 mai. 2023. (n.p.)

uma característica intrínseca das relações de consumo, além de uma presunção legal em favor do consumidor[143].

Ainda quanto à vulnerabilidade do consumidor, Siqueira *et. al.* explicam que é tratada

> [...] como um princípio no ordenamento pátrio, a vulnerabilidade do consumidor está intrinsecamente enquadrada na seara da defesa do consumidor, protegida tanto pela legislação especial, quanto pela imposição que a eleva à categoria constitucional, com a finalidade de constituir a ordem econômica do Estado brasileiro[144].

A literatura apresenta diversos vieses da vulnerabilidade, tal como a vulnerabilidade técnica, científica e fática[145]. No entanto, a ênfase nesse contexto deve ser dada à vulnerabilidade informacional do consumidor.

Feitos os destaques atinentes à vulnerabilidade, deve-se ponderar que, no âmbito do comércio eletrônico, o consumidor acaba por estar em uma situação de agravamento de sua vulnerabilidade. Em outras linhas, no tópico anterior foi mencionado sobre as constantes transformações sociais identificadas a partir do apogeu da internet e do mercado digital, e é importante pontuar que essas mudanças recaem diretamente sobre o consumidor na atualidade, ao passo que o consumidor, via de regra, não está preparado de forma técnica e intelectual para lidar de forma equânime com todas essas mudanças promovidas[146].

Nessa perspectiva, Lehfeld *et. al.* destacam ser:

> [...] imperioso questionar o papel e as características que o consumidor virtual passa a assumir diante de tantas modificações. A partir da falta de informação e despreparo técnica e intelectual do consumidor frente aos negócios pactuados de forma online, busca-se desenvolver uma aplicação da exegese protetiva do Código de Defesa do Consumidor às contratações eletrônicas. Isto porque, embora a relação de consumo permaneça a mesma em sua essência, no comércio eletrônico, o consumidor perde todos os referenciais a que está acostumado, tornando-o ainda mais vulnerável dado o estranhamento tecnológico[147].

Os autores ressaltam, ainda, que "a vulnerabilidade do consumidor no meio eletrônico não deve ser restrita somente à falta de proficiência informática, mas também à ausência de saberes básicos quanto à compreensão da tecnologia utilizada"[148]. Nesse sentido, desde a

---

[143]BEHRENS, Yan West. **Comércio eletrônico de produtos e serviços: uma análise das principais práticas abusivas em prejuízo dos consumidores.** Salvador: Pagince, 2014, p. 309.

[144]SIQUEIRA, . N.; CONTIN,. C.; BARUFI,. B.; LEHFELD,. de S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD . **Revista Eletrônica Pesquiseduca**, [S. l.], v. 13, n. 29, p. 236–255, 2021. DOI: 10.58422/repesq.2021.e1029. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 20 mai. 2023. 2021, p. 242.

[145]MIRAGEM, Bruno. **Curso de Direito do Consumidor**. 6. ed. São Paulo: Revista dos Tribunais, 2016.

[146]SIQUEIRA; CONTIN; BARUFI; LEHFELD, 2021, p. 244.

[147]*Ibidem*, p. 244-245.

[148]*Ibidem*, p. 242.

utilização mais recente da inteligência artificial até as práticas de design que buscam convencer o consumidor a realizar a compra, há muitos pontos de preocupação. Nesse contexto é que entram os dark patterns como práticas que vulnerabilizam ainda mais o consumidor, assunto que será abordado no terceiro capítulo deste estudo.

Em complemento a isso, "com o aprimoramento da internet e as demais adaptações da virtualidade, surgiu o fenômeno do comércio eletrônico, o qual acentuou ainda mais a vulnerabilidade do consumidor"[149]. É que, com toda essa modernização e a forma como as relações sociais e de consumo estão se diferenciando e tomando proporções cada vez mais complexas, a vulnerabilidade que já é tida como uma premissa toma um viés agravado, posto que se aumenta.

Para além das práticas comuns de mercado caracterizadas pela compra de mercadorias ou contratação de serviços em lojas virtuais, o comércio eletrônico engloba ainda os sítios de aproximação, que são "espaços virtuais disponibilizados por empresas para todos os internautas, sejam eles pessoas físicas ou jurídicas, que por intermédio dos serviços de aproximação do sítio, podem comprar ou vender mercadorias"[150].

Nesse âmbito, é mister que se compreenda a construção de alguns cenários cujas implicações jurídicas são evidentes. Inicialmente, destaca-se a dificuldade de se ter real conhecimento das intenções e da lisura da pessoa que está do outro lado da plataforma, e ainda o cenário de descuido dos administradores dos sítios em não estabelecer políticas de segurança eficazes, o que faz com o que o consumidor fique em uma situação de vulnerabilidade agravada ao se expor a riscos[151].

Locatelli e Simon[152] discutem que, para compreender os aspectos jurídicos envolvidos nas relações de consumo em ambientes virtuais, é importante analisar sua dinâmica de funcionamento. Nesses ambientes, a aproximação entre vendedor e comprador é facilitada por um intermediário que administra o site de vendas. Nesse contexto, os interessados em comercializar seus produtos utilizam o site do intermediário, pagando uma taxa percentual sobre as vendas concluídas. O consumidor, ao acessar o site, pode selecionar o produto desejado e, ao manifestar interesse na compra, possibilita-se o contato direto com o vendedor.

---

[149]LOCATELLI, Liliana; DE PAIVA SIMON, Cláudio Antonio. A vulnerabilidade do consumidor ante os ambientes virtuais: o caso dos sítios de aproximação. **Revista Direitos Culturais**, v. 3, n. 4, p. 157-168, 2008, p. 159.
[150]*Ibidem*, p. 158.
[151]*Ibidem*, p. 158-159.
[152]*Ibidem*.

No entanto, esse contato é limitado a informações sobre o produto, preço e condições de pagamento, de modo que outras formas de negociação fora do ambiente do site não são viabilizadas.

Esse modelo de funcionamento vincula o site intermediador à relação contratual, uma vez que ele atua como ponto central de contato e, assim, garante sua participação na conclusão do negócio. Dessa forma, o site de aproximação não apenas facilita a conexão entre comprador e vendedor, mas também assegura que a transação ocorra por meio de sua plataforma, garantindo o recebimento de seu percentual sobre a venda. Isso evidencia a relevância jurídica do intermediário na relação de consumo, já que sua participação direta influencia a forma como as negociações são conduzidas e finalizadas no ambiente virtual.

Cita-se o exemplo dos sítios de aproximação como um dos elementares tipos de desafios enfrentados pelo consumidor. Isso porque os preços praticados nesse tipo de ambiente são, muitas vezes, atrativos, o que faz com que grande parte dos consumidores optem por realizar compras ali.

2.1.3 *A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais*

O reconhecimento da vulnerabilidade do consumidor é essencial para assegurar um equilíbrio nas relações de consumo. Esse entendimento é crucial para promover a igualdade substancial, adaptando a proteção e garantias oferecidas ao consumidor às suas desigualdades específicas. No que diz respeito ao tratamento de dados pessoais em contextos de consumo, Mendes[153] destaca a importância de considerar essa vulnerabilidade, visto que os dados pessoais e as informações derivadas deles representam a pessoa de forma virtual na sociedade. Esta representação pode influenciar significativamente as oportunidades de um indivíduo no mercado, dependendo da forma como esses dados são utilizados.

Neste século, marcado por avanços tecnológicos e inovações, foi possível moldar um perfil de consumo específico através da parametrização e individualização do consumidor, utilizando suas preferências. A produção em massa cedeu espaço à produção personalizada, viabilizada pelo *marketing* direcionado, como observado por Mendes[154]. A vulnerabilidade

[153]MENDES, Laura Schertel Ferreira. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. **Revista de Direito do Consumidor.** Revista dos Tribunais: São Paulo, 2015, p. 6.
[154]*Ibidem*, p. 3.

do consumidor pode ser compreendida de duas formas distintas: (i) a vulnerabilidade técnica, em que o consumidor detém menos informações sobre o fluxo de seus próprios dados; e (ii) a vulnerabilidade fática, que envolve a falta de recursos intelectuais e financeiros para remediar danos oriundos do processamento de dados.

As pessoas têm suas identidades transformadas no ambiente digital, como já mencionado, e esse processo facilita a categorização e manipulação de suas características. Com as diversas ferramentas disponíveis e o constante influxo de informações, os controladores possuem um conhecimento aprofundado sobre o indivíduo, muitas vezes superior ao das pessoas mais próximas a ele, como familiares e amigos, o que gera uma série de ameaças e riscos. Uma infinidade de recursos é empregada diariamente para influenciar suas escolhas e direcionar seus interesses conforme o interesse das grandes marcas, ao passo que definir e ditar padrões de consumo é um processo considerado simples para elas.

O consumidor, identificado como a parte vulnerável na relação de consumo, enfrenta restrições no controle sobre o fluxo de seus dados e informações pessoais no mercado. Além disso, ele encontra dificuldades em implementar medidas eficazes para se proteger dos riscos associados ao processamento desses dados[155]. Dentro deste cenário de vulnerabilidade, a economia do consumo tem adotado um modelo mais flexível, focado na personalização, assegurando que o consumidor, uma vez individualizado através de seus dados pessoais, tenha acesso a produtos que correspondam exatamente aos seus desejos. A respeito disso, a literatura destaca que,

> Para se atingir tanto a diferenciação da produção, quanto a diferenciação do marketing, faz-se necessária a coleta massiva de informações sobre os consumidores, seus hábitos e comportamentos. Assim, as empresas adquirem a capacidade de ofertar produtos especializados, singularizados e altamente qualificados, em função do mercado e do consumidor, bem como de direcionar-lhe a sua publicidade[156].

Para a efetivação dessa personalização, o atual modelo de mercado estabelece uma interação entre a sociedade da informação e a sociedade contemporânea de consumo, conforme explica Mendes[157]. Neste modelo, um segmento fornece os dados pessoais coletados, enquanto o outro utiliza esses dados para personalizar produtos e serviços. Esse sinergismo sugere uma maior eficácia nas vendas, mas também apresenta desafios

[155]MENDES, 2015, p. 3.
[156]*Ibidem*, p. 3.
[157]*Ibidem*, p. 3.

significativos. Além disso, há uma preocupação particular com a exclusão do consumidor dos mercados, um tema sensível que merece atenção.

Conforme abordado anteriormente sobre a "vida na sociedade da vigilância", nas palavras de Stéfano Rodotá, essa realidade é bastante relevante no contexto atual, visto que a vigilância permite "classificar pessoas em categorias baseadas na avaliação de seus riscos e discriminar o acesso a certos bens e serviços, impactando significativamente suas oportunidades de vida"[158]. Neste contexto, o consumidor enfrenta a diminuição de sua autodeterminação, muitas vezes por não conhecer como seus dados são utilizados ou até mesmo por desconhecer que eles estão sendo tratados, evidenciando mais uma vez falhas no consentimento. Como resultado,

> [...] o consumidor está sujeito ao risco de ser discriminado indevidamente no mercado de consumo, caso tenha negado acesso a bens e serviços no mercado de consumo ou tenha as suas chances de vida diminuídas, em razão das informações armazenadas em bancos de dados e utilizadas de forma discriminatória[159].

A vulnerabilidade do consumidor no contexto da coleta e processamento extensivos de dados é inquestionável. A literatura até cunha o termo "consumidor de vidro" para descrever essa situação de fragilidade na qual o consumidor se encontra em relação ao mercado. Isso se dá em um cenário onde "inúmeras empresas tomam decisões e influenciam as oportunidades de vida do consumidor, baseadas nas informações pessoais armazenadas em bancos de dados"[160].

2.2 A obtenção do consentimento do titular de dados pessoais

2.2.1 *Consentimento do titular de dados pessoais na literatura*

O consentimento é um dos elementos cardeais da Lei Geral de Proteção de Dados Pessoais brasileira[161]). Isso porque a arquitetura regulatória da referida lei tem como premissa a obtenção do consentimento válido do titular para a feitura de qualquer um dos atos que envolvam os seus dados pessoais, coleta, tratamento, armazenamento etc.

---

[158]MENDES, 2015, p. 5.
[159]*Ibidem*, p. 5.
[160]*Ibidem*, p. 6.
[161]BIONI, Bruno. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento**. In: Minha Biblioteca, (3rd edição). Grupo GEN, 2021, p. 127.

Na busca por elaborar um percurso para o consentimento no cenário brasileiro, desde 2010 até o ano de publicação da LGPD, em 2018, Bruno Bioni menciona que,

> [...] na primeira versão do anteprojeto de lei colocado sob consulta pública em 2010, o consentimento era, em termos topográficos, a única base legal para o tratamento de dados pessoais. Isso se repetiu na segunda consulta pública em 2015, quando o que hoje são as demais bases legais da LGPD eram hipóteses nas quais o consentimento poderia ser dispensado[162].

Desse modo, observa-se que, desde o esboço da LGPD, o consentimento é o seu cerne. Além disso, nota-se no conteúdo atual da norma uma preocupação verdadeira com a participação do titular na gerência de suas informações pessoais. Isso demonstra-se na essência de sua concessão, já que "deve ser livre, inequívoco e dizer respeito a uma finalidade determinada de forma geral, e em determinados casos, deve ser, ainda, específico"[163].

Bioni também ressalta que

> [...] grande parte dos princípios tem todo o seu centro gravitacional no indivíduo: a) de um lado, princípios clássicos, como a transparência, a especificação de propósitos, de acesso e qualidade de dados por meio dos quais o titular do dado deve ser munido com informações claras e completas sobre o tratamento de seus dados e, ainda, ter acesso a eles, para, eventualmente corrigí-los; b) de outro lado, princípios mais "modernos", como adequação e necessidade, em que o tratamento dos dados deve corresponder às legítimas expectativas do seu titular. Isso deve ser perquirido de acordo com a finalidade específica para o tratamento dos dados, assegurando-se que os dados sejam pertinentes, proporcionais e não excessivos (minimização dos dados)[164].

A suma do consentimento na LGPD é permitir que o titular de dados não apenas participe dos atos de coleta, processamento, e outros, que envolvem os seus dados pessoais, mas que ele tenha gerência e controle sobre esse processo, sendo-lhe permitido anuir e revogar o consentimento quando assim entender pertinente.

Assim, pode-se dizer que o ponto alto da abordagem brasileira à proteção de dados é a necessidade de obter o consentimento do titular dos dados. A legislação pátria já incorpora o princípio da transparência, que exige a clareza e precisão na informação, seja sobre produtos, serviços e, agora, sobre a coleta de dados. Logo, ao coletar dados, é essencial obter o consentimento do titular, que deve estar fundamentado em informações claras e inequívocas sobre os propósitos da coleta e o destino dos dados. Essas informações devem ser fornecidas de maneira clara e precisa.

---

[162]BIONI, 2021, p. 127
[163]*Ibidem*, p. 127.
[164]*Ibidem*, p. 128.

A seção I do capítulo II da lei estabelece os critérios para o processamento de dados pessoais, esclarecendo que tal atividade só pode ocorrer com o consentimento do titular (art. 7°, I). Além disso, a lei especifica que o acesso aos dados pessoais deve ser público, levando em conta a finalidade, a boa-fé e o interesse público que justificam sua divulgação[165] (art. 7°, § 3°).

Quanto ao método de obtenção do consentimento, a lei determina que este deve ser expresso por escrito ou por qualquer outro meio que comprove a manifestação de vontade do titular. Se for por escrito, deve estar em uma cláusula contratual destacada das demais (art. 8° e parágrafos)[166]. Gisela Pimenta Gadelha[167], na linha do que estabelece a legislação, enfatiza que o controlador é responsável por provar que obteve o consentimento do titular. Ela também explica que a cláusula de consentimento, especialmente em um contrato, deve ser clara quanto à finalidade específica e determinada.

Conforme o art. 8°, § 4°, é importante ressaltar que consentimentos vagos ou autorizações genéricas para o processamento de dados pessoais são nulos, resultando na responsabilização do controlador por utilizar dados pessoais sem consentimento adequado[168].

O consentimento do consumidor é fundamental para que ele possa exercer seu direito à autodeterminação informativa, como destaca Mendes, uma vez que é por meio dele que o indivíduo autoriza ou recusa o processamento de seus dados pessoais. A autora ressalta que "esse mecanismo é a maneira do direito assegurar a autonomia privada do cidadão"[169]. Assim, o processamento de dados depende da aprovação ou rejeição do usuário, neste caso, o consumidor.

No entanto, é importante considerar a forma como esse consentimento é obtido, pois pode existir vício na maneira como foi solicitado pelo controlador ou operador. Assim, o consumidor tem o direito de revogar seu consentimento e a legislação prevê outras sanções legais aplicáveis aos infratores. Para Mendes[170], a questão do consentimento deve ser

---

[165]BRASIL, **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. (n.p.)
[166]*Ibidem*.
[167]GADELHA, Gisela Pimenta. **Boas práticas e governança corporativa**. in: Manual do DPO. São Paulo: Thomson Reuters Brasil, 2021, p. 197.
[168]BRASIL, **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. (n.p.)
[169]MENDES, 2015, p. 7.
[170]*Ibidem*, p. 9.

interpretada à luz da boa-fé objetiva, que implica um diálogo entre a LGPD (art. 6°, caput) e o CDC (art. 4°, III, e art. 51, IV).

A Lei Geral de Proteção de Dados Pessoais destaca a importância da boa-fé no tratamento de dados pessoais, estabelecendo um padrão de comportamento que se alinha à ideia de boa-fé objetiva. Ao incorporar este princípio, a lei impõe um dever geral de conduta que visa proteger a confiança nas relações de consumo. A boa-fé objetiva é reconhecida como uma cláusula geral que cria obrigações acessórias além da obrigação principal, moldando a conduta dos agentes envolvidos.

Segundo Carvalho[171], a cláusula geral de boa-fé, adotada pelo Código de Defesa do Consumidor, serve como um mecanismo para definir a abusividade no exercício dos direitos. Essa abordagem flexibiliza o sistema consumerista e estabelece, dentro do arcabouço legal, uma série de deveres associados às relações contratuais, contribuindo assim para uma regulação mais abrangente e adaptada às complexidades das relações de consumo contemporâneas.

A proteção dos dados pessoais dos consumidores destaca sua vulnerabilidade em relação ao tratamento dessas informações, tornando fundamental a responsabilidade dos controladores de dados. Esses agentes, que são responsáveis por coletar, armazenar e processar dados pessoais, possuem o dever de garantir a segurança das informações sob sua guarda. Nesse contexto, emergem os deveres de cooperação e cuidado, fundamentados no princípio da boa-fé objetiva, o que exige do controlador uma conduta íntegra e honesta no manejo desses dados. Além disso, o dever de diligência destaca-se como uma obrigação crucial, reforçando a necessidade de uma gestão cuidadosa e responsável dos dados pessoais dos consumidores, garantindo que sejam tratados conforme a finalidade para a qual foram coletados[172].

No âmbito da Lei Geral de Proteção de Dados (LGPD), a boa-fé objetiva exerce um papel essencial ao fundamentar a tutela das expectativas legítimas do titular de dados frente ao controlador. Como disposto no artigo 10, inciso II, da LGPD, essas expectativas são formadas a partir das circunstâncias concretas em que o consentimento foi dado, da finalidade informada para o uso dos dados e da maneira como as informações prévias foram

[171]CARVALHO, Diógenes Faria de. **A boa-fé objetiva nos contratos de consumo.** Dissertação apresentada como requisito para a conclusão do Mestrado em Direito das Relações Econômico-Empresariais. Universidade de Franca - UNIFRAN: São Paulo, 2006.

[172]MIRAGEM, Bruno Nubens Barbosa. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor**. São Paulo: Revista dos Tribunais, 2019, p. 5.

compreendidas pelo titular[173]. Nesse sentido, a tutela da confiança do consumidor envolve não apenas a credibilidade nas informações prestadas pelo controlador, mas também a garantia de que o uso dos dados respeitará o que foi informado no momento do consentimento.

Assim, a confiança depositada pelo consumidor no controlador exige que este atue de forma consistente com as informações inicialmente prestadas, sem adotar comportamentos que contrariem a finalidade para a qual os dados foram coletados. O princípio da boa-fé objetiva impõe que os controladores de dados respeitem essa vinculação, evitando qualquer conduta que possa prejudicar o titular ou desviar os dados de seu propósito original[174]. Dessa forma, a gestão de dados pessoais demanda não apenas transparência e honestidade, mas também uma postura de respeito à finalidade declarada e às expectativas legítimas do consumidor.

Consequentemente, ao consumidor é assegurado o direito de ter suas expectativas legítimas atendidas. Além disso, para proteger esse direito, como já foi mencionado, existe a possibilidade de o consumidor revogar o consentimento previamente dado, interrompendo assim o processamento dos seus dados. Em situações em que os agentes responsáveis pelo tratamento de dados violam o princípio da boa-fé, estão sujeitos a penalidades.

O avanço tecnológico que tem intensificado a exploração e utilização de dados pessoais em seus diversos processos, somado ao crescente domínio das grandes empresas no mercado, acentuou a vulnerabilidade dos consumidores, conforme demonstrado. Portanto, é crucial reconhecer e assegurar a proteção abrangente de seus direitos, conforme estabelecido pelo Código de Defesa do Consumidor.

2.2.2 *Proteção de dados pessoais como um direito básico do consumidor*

Mendes[175] destaca a importância de considerar a vulnerabilidade do consumidor quanto ao tratamento de dados pessoais realizados no âmbito das relações de consumo. Além disso, observam-se situações que colocam em risco os consumidores devido ao processamento de seus dados, que podem incluir desde a categorização até a exclusão do

[173]BRASIL, **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. (n.p.)
[174]MIRAGEM, 2019, p. 5.
[175]MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental.** Ed. Saraiva: São Paulo, 2014, p. 198.

mercado de consumo, afetando negativamente seu acesso a bens de consumo e oportunidades sociais.

Com o aumento do uso de dados pessoais pelas empresas para fomentar o consumo, a vulnerabilidade do consumidor torna-se mais acentuada. Portanto, é essencial garantir a proteção da personalidade, privacidade e dados pessoais do consumidor. A literatura especializada ressalta a necessidade de proteger esses direitos fundamentais, destacando sua relevância no contexto atual, nos seguintes termos:

> A partir da vivência institucional da defesa do consumidor e do desenvolvimento jurisprudencial analisado, entendemos que a concretização do dever de proteção do consumidor numa sociedade da informação somente pode ser atingida com o reconhecimento de um direito básico do consumidor à proteção de dados pessoais. Este nada mais é do que o reflexo, no âmbito infraconstitucional, do direito fundamental à inviolabilidade da intimidade e da vida privada (art. 5°, X), na sua dimensão da proteção de dados pessoais. Afinal, como previsto pelo próprio art. 7° do CDC, o catálogo de direitos básicos não é numerus clausus, possibilitando o reconhecimento dos outros direitos "decorrentes de tratados e convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivam dos princípios gerais do direito, analogia, costumes e equidade". Ademais, o art. 43 do CDC e o art. 21 do CC reforçam o reconhecimento desse direito básico do consumidor[176].

Existem duas dimensões cruciais na proteção de dados dos consumidores: a primeira é a salvaguarda da personalidade contra os riscos associados ao manuseio de dados, abrangendo desde a coleta até a sua disseminação no mercado. A segunda dimensão envolve o empoderamento do consumidor, permitindo que, através da autodeterminação, ele possa gerir seus próprios dados na sociedade. Mendes[177] assim explica:

> Como se percebe, o preceito elaborado envolve tanto um aspecto subjetivo (controle dos dados pessoais pelo próprio consumidor), quanto um aspecto objetivo (proteção contra os riscos causados pelo tratamento de dados pessoais). A importância das duas dimensões é fundamental para possibilitar a autodeterminação informativa do consumidor, ao mesmo tempo que propicia um controle objetivo de legitimidade do tratamento de dados pessoais. Esse controle objetivo torna-se ainda mais relevante no mercado de consumo, em que a discrepância de poderes e de informações entre consumidores e fornecedores é tão grande que dificulta ao consumidor a tomada de decisão livre e informada a respeito do fluxo de seus dados. Não obstante, tal conceito não reduz a autonomia do consumidor no controle de seus dados; ao contrário, trata-se de garantir sua liberdade efetiva, a partir da verificação do respeito à boa-fé objetiva e às suas legítimas expectativas.

Portanto, é vital garantir uma informação clara e específica sobre a coleta e o tratamento de dados pessoais, essencial para o processo de autodeterminação informativa do titular, neste caso, o consumidor. Respeitar a boa-fé objetiva implica cumprir com os deveres

---

[176]MENDES, 2015, p. 14.
[177]*Ibidem*, p. 14.

anexos de conduta, significando que os responsáveis pelo tratamento de dados devem cooperar com o titular, fornecendo informações completas sobre a manipulação dos dados e os propósitos do seu tratamento. Além disso, devem assegurar o uso dos dados exclusivamente para os fins declarados e protegê-los contra acessos não autorizados.

Mendes[178] ressalta que o Código de Defesa do Consumidor foi um dos primeiros a reconhecer a privacidade como um direito básico, estabelecendo uma proteção abrangente do consumidor em vários aspectos, desde sua personalidade até seus interesses econômicos. Com o caráter principiológico de suas normas, foi possível adaptá-las para lidar com os avanços tecnológicos, inclusive no processamento de dados, oferecendo proteção aos consumidores também nesse aspecto.

Para uma proteção efetiva dos dados como um direito básico do consumidor, é essencial o diálogo entre o Código de Defesa do Consumidor e a LGPD, com foco especial no consentimento e na finalidade do uso dos dados. Mendes[179] sugere a adoção de procedimentos conhecidos como "*Fair Information Principles*", que são encontrados em diversas legislações, tratados e instrumentos internacionais, como uma forma de garantir o direito do consumidor à proteção de seus dados.

O primeiro procedimento essencial mencionado é a transparência. Espera-se que o controlador de dados informe ao consumidor sobre como a coleta é realizada, o processo de tratamento, os objetivos, os tipos de dados processados e a duração da conservação desses dados em suas bases. Essas informações devem ser fornecidas ao consumidor antes da coleta, e a clareza e precisão dessas informações são fundamentais para um consentimento válido. Em outras palavras, o consentimento do consumidor deve ser obtido somente após a apresentação dessas informações, para que seja considerado legítimo. Há também uma obrigação específica para os controladores de dados que operam *on-line*, que consiste em disponibilizar "termos de privacidade" em suas páginas, contendo todas as informações já mencionadas.

O segundo procedimento enfoca a necessidade de compatibilidade entre o tratamento de dados e a finalidade da coleta. Isso significa que as informações coletadas do consumidor não devem ser usadas para propósitos diferentes daqueles inicialmente estabelecidos. Mendes[180] ressalta que esse princípio é fundamental para assegurar que os dados não sejam

[178]MENDES, 2015, p. 13.
[179]MENDES, 2014.
[180]*Ibidem*, 2014, p. 216.

usados fora de contexto, evitando riscos e danos ao consumidor. O princípio da finalidade assegura que, em obediência à razoabilidade e adequação, os dados do consumidor sejam utilizados apenas para os fins para os quais foram coletados, sendo qualquer desvio considerado abusivo e uma violação do consentimento.

O terceiro procedimento é o direito de acesso, retificação e cancelamento. Esse direito reforça a capacidade de controle do titular sobre seus dados pessoais, sendo fundamental que tal direito seja assegurado ao consumidor como meio de equilibrar a relação de consumo. A possibilidade de revogação do consentimento, ou seja, o direito de cancelar a concessão dos dados, confere ao consumidor domínio sobre seus dados. Essa medida é crucial para a efetividade da autodeterminação informacional, como enfatiza Mendes[181].

O quarto procedimento crucial é a proteção aprimorada de dados sensíveis. Conforme definido no art. 5°, II, da LGPD, dados sensíveis são aqueles que podem levar à discriminação do consumidor[182]. Dessa forma, é essencial oferecer uma proteção especial a esses dados para prevenir tratamentos desiguais e discriminatórios no mercado de consumo, evitando a exclusão do consumidor. É importante ressaltar que o tratamento de dados pessoais sensíveis deve seguir as condições específicas estabelecidas pela legislação, como indicado no art. 11 da LGPD.

O quinto procedimento envolve assegurar a segurança dos dados pessoais. Os controladores de dados e todos os envolvidos no processo de tratamento têm a responsabilidade de proteger essas informações. Isso implica em armazenar os dados cuidadosamente e prevenir violações. Tal dever pode ser visto como uma obrigação de cuidado ou diligência, um aspecto da boa-fé objetiva, garantindo que o indivíduo esteja protegido contra a violação de seus dados, uma vez que confiou no controlador. Verbicaro e Vieira discutem esse aspecto, destacando a importância desse dever na proteção de dados pessoais:

> [...] a irregularidade no uso dos dados está vinculada à segurança da proteção informacional. A adoção de medida de segurança para evitar acessos não autorizados é de essencial importância no trabalho dos agentes. A LGPD estabelece medidas de proteção contra o tratamento inadequado e ilícito dos dados, tendo os agentes o dever de zelar pelos dados, desde a sua concepção até o término do tratamento e sua exclusão "podendo a autoridade nacional dispor sobre padrões técnicos mínimos, considerando a natureza das informações, as características específicas do tratamento e o estado atual da tecnologia, especialmente, no caso de dados pessoais sensíveis. Em caso de incidente de segurança que afete os dados

[181]MENDES, 2014, p. 217.

[182]BRASIL, **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. (n.p.)

> processados, o agente de dados deve informar a autoridade nacional no prazo razoável[183].

De acordo com o artigo 46 da Lei Geral de Proteção de Dados Pessoais, é responsabilidade dos agentes de tratamento assegurar a segurança dos dados pessoais, incluindo a proteção contra acessos não autorizados de terceiros[184]. Se ocorrer uma violação dessa obrigação, isso representa não apenas uma falha no cumprimento do dever de cuidado, evidenciando uma quebra na boa-fé objetiva, mas também uma infração à legislação por não manter um sistema de segurança suficientemente robusto para prevenir acessos não autorizados.

A legislação exige, portanto, que os agentes de tratamento implementem medidas de segurança eficazes para proteger os dados pessoais de acessos indevidos. Esse requisito visa obrigar os agentes a reforçarem seus sistemas de segurança, reduzindo as chances de violações de dados por terceiros, como hackers, que podem comprometer desde a privacidade e intimidade do indivíduo até a segurança de informações armazenadas, como fotos e conversas privadas.

O risco associado ao compartilhamento indevido de dados pessoais na era pós-moderna está diretamente relacionado à proteção da personalidade do indivíduo. Além da privacidade, direitos como o de imagem, intimidade e sossego podem ser violados em caso de vazamento de dados. Mesmo com o dever de segurança sendo central nas práticas de governança e nas obrigações impostas por órgãos reguladores, os controladores de dados precisam adotar cuidados adicionais. Medidas como a implementação de acessos restritos, uso de senhas complexas e *tokens*, criptografia e investimentos significativos em sistemas de segurança da informação são essenciais para quem lida com o processamento de dados pessoais.

Domingo Montanaro[185] destaca a importância de criar uma cultura focada em segurança da informação nas empresas. Além de simplesmente detectar tentativas de violação, é essencial que cada uma delas seja sistematicamente frustrada. Com o avanço da tecnologia, já é possível antever riscos e, por conseguinte, prevenir danos. Assim, a tecnologia da informação deve ser utilizada como um mecanismo automatizado, integrado e inteligente para

---

[183]VERBICARO, Dennis; VIEIRA, Janaína. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. **Revista de Direito do Consumidor**: São Paulo, 2021, p. 12.

[184]BRASIL, **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD)**. (n.p.)

[185]MONTANARO, Domingo. **Medidas técnicas e administrativas para a segurança da informação**. In: Manual do DPO – Data Protection Officer. São Paulo: Revista dos Tribunais: 2021, p. 115.

proteger as informações. Isso implica que, ao garantir a segurança dos dados, as empresas têm o dever de diligência de implementar sistemas de *compliance* para estruturar uma abordagem preventiva interna e estabelecer protocolos para evitar falhas nas cadeias de segurança de dados.

O sexto e último procedimento proposto por Mendes[186] é a limitação temporal dos dados, segundo a qual "os dados não devem ser armazenados por mais tempo do que o necessário para cumprir o propósito da coleta". Esse princípio garante ao consumidor que suas informações não serão retidas indefinidamente nos bancos de dados, evitando danos potenciais a longo prazo. De acordo com Mendes, o contexto específico determinará o período adequado para o tratamento de dados, considerando os "riscos, benefícios e sensibilidade do tratamento"[187].

A efetiva proteção dos dados pessoais pelo poder público, atuando como fiscalizador e defensor dos direitos do consumidor conforme a Constituição (art. 5°, XXXII)[188], pode ser complementada pela atuação proativa do setor privado. Embora os órgãos reguladores desempenhem um papel fundamental na proteção dos direitos dos consumidores, há um espaço para inovação e implementação de soluções criativas. Lidar com as complexas demandas sociais é um desafio e, para isso, iniciativas como a autorregulação regulada são apropriadas. Neste modelo, o setor privado desenvolve estratégias para resolver problemas específicos de cada nicho regulado, sob supervisão e cooperação do setor público, por meio de normas e protocolos de governança.

Sob essa ótica, o setor privado tem um papel fundamental em colaborar com a defesa do consumidor, particularmente no que tange à proteção de dados. Iniciativas como a formação de grupos de trabalho e fóruns dedicados a essas questões, bem como o estabelecimento de sistemas e certificações de controle de qualidade, são essenciais para efetivar as garantias constitucionais e legais de proteção ao consumidor. A Autoridade Nacional de Proteção de Dados desempenha um papel importante de facilitadora de diálogo e orientação, incentivando as empresas a se organizarem em seus respectivos setores para um diálogo produtivo e eficiente.

---

[186]MENDES, 2014, p. 220.
[187]*Ibidem*, p. 220.
[188]BRASIL. **Constituição Federal de 5 de outubro de 1988**. (n.p.)

3 PADRÕES OBSCUROS E SEUS IMPACTOS NA VALIDADE DO CONSENTIMENTO PARA A COLETA DE DADOS PESSOAIS

3.1 Padrões obscuros e consentimento válido

3.1.1 *Padrões obscuros, conceito e desdobramentos*

A mesa redonda da OCDE conceituou padrões obscuros como "interfaces de usuários usadas por algumas empresas online para levar os consumidores a tomarem decisões que de outra forma não teriam tomado se estivessem totalmente informados e capazes de selecionar alternativas", baseando-se no conceito de Mathur e Ksirsagar[189]. Assim, os padrões obscuros podem ser entendidos como práticas que induzem o indivíduo a fazer algo que ele não tinha inicialmente a intenção de fazer, mas acaba sendo convencido em um processo de condução.

Os padrões obscuros são usados em grande parte por sites de compras on-line globais e estão presentes em mais de 95% dos 200 aplicativos mais utilizados pelas pessoas[190]. Nota-se, a partir desses dados, que a sua utilização é mais corriqueira do que a discussão a seu respeito, dado que no Brasil atualmente o debate sobre o assunto é ainda incipiente.

A identificação dos padrões obscuros é um desafio, bem como a resistência e o combate a eles. Eles são capazes de diminuir a autonomia das pessoas, contribuindo para a redução do seu bem-estar social e da confiança que elas depositam no ambiente online, causando um cenário de insegurança[191].

Ainda que haja um esforço por se adequar por parte dos agentes de mercado às normas de proteção de dados pessoais, o efetivo cumprimento é pouco visto. Nota-se que em alguns casos as políticas de privacidade e termos de uso expostos ao usuário no momento da obtenção de seu consentimento funcionam apenas como uma forma de "isenção de responsabilidade para as empresas, sem de fato explicar especificamente como os dados são usados ou combinados para gerar outras informações"[192].

---

[189]MARQUES, Cláudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. Dark patterns e padrões comerciais escusos. **Revista de Direito do Consumidor.** vol. 145. ano 32. p. 295-316. São Paulo: Ed. RT, jan./fev. 2023. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/174455. Acesso em: 05 mai. 2024. 2023, p. 296.

[190]*Ibidem*, p. 296.

[191]*Ibidem*, p. 296.

[192]LIMA, Patrícia Raposo Santana; DE CASTRO SALGADO, Luciana Cardoso. Estratégias de comunicação do Consentimento Informado e rastros de Padrões Obscuros no Instagram. In: **Anais do III Workshop sobre as Implicações da Computação na Sociedade.** SBC, 2022. p. 45.

Antes de adentrar especificamente na conceituação de *dark patterns*, mostra-se importante trazer um breve panorama histórico sobre tais práticas. A manipulação dos usuários não é algo ligado unicamente ao digital. As grandes lojas de varejo empregam esse tipo de prática há muitos anos. Como exemplo, cita-se a utilização de táticas de falsas promoções[193].

Jordyn Michaels explica que, a partir da década de 1970, pesquisadores focados em aspectos comportamentais da economia lançaram diversos estudos sobre as ações irracionais tomadas pelos consumidores no momento de aquisição de bens. Durante essas pesquisas, identificou-se que a ausência de conhecimento sobre fatores de mercado impactava diretamente nas más escolhas feitas pelos cidadãos, de modo que se iniciou a prática de diversos testes que visavam reforçar esses aspectos[194].

A aplicação de práticas que visassem influenciar os consumidores na tomada de decisões de consumo foi denominada como "*nudging*" ou "nudge", que será melhor detalhado adiante. No ano de 1996, de acordo com Jordyn Michaels, tais táticas foram utilizadas no mundo digital pela primeira vez. A empresa Hotmail começou a inserir ao final de cada e-mail enviado pelos usuários através de sua plataforma uma frase indicando que os receptores poderiam adquirir um endereço eletrônico grátis com a companhia[195].

Isso fazia com que os usuários da plataforma, sem qualquer tipo de consciência plena sobre o fato, passassem a fazer propagandas gratuitas para a Hotmail sempre que enviassem um e-mail, prática que foi um enorme sucesso[196]. Esses parecem ter sido os primórdios do que denominamos hoje como *dark patterns* ou padrões obscuros.

Os padrões obscuros surgem de uma convergência de práticas consolidadas em diferentes áreas, como o varejo, a economia comportamental e o *growth hacking* . No varejo, estratégias como preços psicológicos estabelecem uma base para manipulações sutis de comportamento. A economia comportamental contribuiu com conceitos como o nudge, mencionado anteriormente, originalmente desenvolvido para ajudar indivíduos a tomar decisões benéficas, mas que, no ambiente digital, está sendo utilizado de modo a manipular a tomada de decisão dos indivíduos, geralmente em relação a compras on-line e assinaturas em

---

[193]LUKOFF, Kai; HINIKER, Alexis; GRAY, Colin M.; MATHUR, Arunesh; CHIVUKULA, Shruthi. **What can CHI Do About Dark Patteens?**. In: CHI '21 Extended Abstracts. Japão, 2021, p. 2.

[194]MICHAELS, Jordyn. **Pathways to the Light: Realistic Tactics to Address Dark Patterns.** Rutgers Computer and Technology Law Journal 49, n. 1: Chicago, p. 176 a 206, 2022, p. 177.

[195]*Ibidem*, p. 179.

[196]*Ibidem*, p. 178.

geral. Por fim, o *growth hacking*, focado no crescimento rápido e na monetização de serviços, refina essas práticas através de experimentos constantes, como testes A/B, para maximizar resultados e explorar habilidades cognitivas dos usuários[197].

Essas práticas não visam apenas aumentar os lucros, mas também coletar dados e prender a atenção dos usuários. Consentimentos para rastreamento, formulados de maneira confusa, ilustram como a privacidade dos indivíduos é comprometida puramente. Além disso, ao tornar plataformas viciantes, as empresas prolongam a interação com seus serviços, o que aumenta tanto as oportunidades de monetização quanto a coleta de informações pessoais. O impacto dessas práticas vai além do campo econômico, atingindo valores fundamentais como a autonomia e a confiança dos consumidores no ecossistema digital[198].

O termo *dark pattern* foi utilizado pela primeira vez, no ano de 2010, pelo designer Harry Brignull. O mencionado especialista definiu que padrões obscuros estariam conectados à aplicação de truques nas interfaces digitais para que os usuários tomem decisões que não teriam intuito, como a assinatura de algum programa[199]. Atualmente, inexiste um conceito único para *dark patterns*. Entretanto, levando em consideração as definições adotadas por Claudia Lima Marques, Laura Schertel Mendes e Laís Bergstein, é possível perceber alguns exemplos do que se pode entender como padrões obscuros.

O primeiro exemplo atribuído pelas mencionadas autoras seria a adição de itens na cesta dos consumidores sem que haja um consentimento do usuário na aquisição de tais produtos. Isso pode ocorrer por meio de uma aplicação no estilo *opt-out* ou de uma caixa de seleção em alguma página anterior acessada pelo consumidor[200]. Outra prática listada seria a denominada isca e troca. Nesse formato, o usuário, por meio de uma ação, acaba desencadeando um resultado indesejável que envolve custos adicionais. São inseridos valores extras quando o consumidor está finalizando a aquisição de produtos, por exemplo. Também é possível que sejam empregadas táticas de continuidade forçada de assinatura de bens ou de serviços, através da aplicação de uma falsa taxa única ou de um período de teste grátis.

Podem ser adotadas táticas de escassez que fazem com que o consumidor se engane sobre a existência de mais ou menos produtos em estoque. Na interface do site são inseridas

---

[197] NARAYANAN, Arvind; MATHUR, Arunesh; CHETTY, Marshini; KSHIRSAGAR, Mihir. **Dark Patterns: Past, Present, and Future: A evolução de interfaces de usuário complicadas**. V. 18, n. 2, p. 67-92, mar./abr. 2020. Disponível em: https://doi.org/10.1145/3400899.3400901. Acesso em: 08 nov. 2024. p. 72.
[198] *Ibidem.* p. 72.
[199] MICHAELS, 2022, p. 178.
[200] MARQUES; MENDES; BERGSTEIN, 2023, p. 296.

informações de que em breve determinada oferta se esgotará ou que o consumidor detém um prazo limite para finalização da compra. Essas práticas podem também se relacionar ao uso da emoção para que o consumidor realize determinada ação que não deseja.

Claudia Lima Marques, Laura Schertel Mendes e Laís Bergstein citam, ainda, práticas de *"confirmshaming",* perguntas enganosas ou venda sob pressão. As ações se relacionam à adoção de métodos para culpar, pressionar ou enganar o usuário na aquisição de determinado produto ou de bens relacionados ao que o consumidor já visava adquirir.

Nesse aspecto, cita-se as táticas que dificultam o cancelamento de serviços ou bens adquiridos pelos consumidores. As referidas autoras explicam que, no Brasil, é fácil para que os usuários se inscrevam para utilizar determinada atividade, já a finalização das assinaturas é uma atividade que consome uma quantidade de tempo desproporcional.

Em 2021, o Conselho Norueguês do Consumidor indicou que a Amazon utilizaria padrões obscuros para promover o serviço de assinatura da empresa, denominado "amazon prime". A plataforma conteria diversos obstáculos que impediriam que os consumidores cancelassem a inscrição nos mencionados serviços. Seriam exemplos de tais *dark patterns* introduzidos pela companhia: existência de uma interface complexa e com muitos passos, adição de textos enganosos e a necessidade de resposta de, ao menos, quatro perguntas idênticas antes de finalização do processo[201].

Mark Leiser[202] explica que o Facebook introduziu padrões obscuros que fazem com que os usuários da plataforma compartilhem mais informações pessoais do que deveriam. São introduzidas mensagens sobre a política de privacidade da companhia, que só permite que os cidadãos escolham entre aceitar os termos definidos ou conhecer mais sobre as práticas adotadas pela empresa, o que dificulta que o navegante consiga discordar de determinada ação.

Claudia Lima Marques, Laura Schertel Mendes e Laís Bergstein apontam, por fim, a adoção de mensagens automáticas, que podem chamar a atenção do consumidor para determinado serviço, o uso de testemunhos incertos sobre determinados bens que iludem o

[201]LEISER, Mark. **Illuminating Manipulative Design: From "Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive.** Loyola Consumer Law Review, v. 34, p. 484-528, 2022, p. 491.
[202]*Ibidem*.

consumidor a adquiri-los, a implementação de sistemas que dificultem uma pesquisa de preços e anúncios disfarçados como outras aplicações que induzam o acesso[203].

No ano de 2012, a Autoridade de Padrões de Publicidade Norte-Americana ordenou que o TripAdvisor, um site sobre experiências e viagens, reescrevesse mais de cinquenta milhões de comentários inseridos na plataforma. Tal determinação levou em consideração que o site fazia com que os usuários acreditassem que diversas resenhas eram de viajantes reais ou genuínos, quando, em verdade, tratava-se de propaganda[204].

Harry Brignull, o precursor do termo *dark pattern*, criou um site para listagem e disseminação de conhecimento sobre o tema. Inicialmente, a plataforma foi denominada como "darkpatterns.org", contudo, no ano de 2022, o site foi renomeado como "deceptive patterns". O pesquisador estabelece uma classificação dos padrões obscuros em dezesseis tipos diferentes[205].

Além dos exemplos apresentados por Claudia Lima Marques, Laura Schertel Mendes e Laís Bergstein, o pesquisador Harry Brignull apresenta a prática de "nagging". De acordo com o mencionado designer, a tática consiste na inserção pelas plataformas digitais de mensagens automáticas que evitem que o usuário tome determinada ação por meio da interrupção do que estava sendo realizado anteriormente.

Seria a inclusão de uma espécie de barreira que dificultaria que os usuários continuem executando ações que não seriam do interesse das plataformas digitais. Harry Brignull aponta, ainda, a possibilidade de uma pré-seleção ou um ocultamento das opções disponíveis ao consumidor pelo site, o que impactaria diretamente na tomada de decisões pelos cidadãos.

Mark Leiser apresenta uma classificação para os padrões obscuros levando em consideração os efeitos de tais práticas nos consumidores. A primeira divisão seria a de táticas de coerção que intimidam ou obrigam os usuários a tomarem alguma ação, seja por meio de preenchimento obrigatório ou por meio do envio de mensagens intimidadoras[206].

A segunda seria a aplicação de interfaces que confundam o usuário, como a inserção de perguntas que, mesmo que respondidas em sentido contrário pelo consumidor, engatilham outros questionamentos no mesmo formato. Há, ainda, práticas de distração que buscam

---

[203]MARQUES; MENDES; BERGSTEIN, 2023, p. 297.
[204]LEISER, *op. cit.*, p. 498.
[205]BRIGNULL, Harry. **Types of deceptive pattern.** Disponível em: https://www.deceptive.design/types. Acesso em: 31 ago. 2024.
[206]LEISER, 2022, p. 501.

desconcentrar o navegante de determinada ação para direcioná-lo à alguma prática que seja vantajosa para o site.

A quarta seria a exploração de erros dos usuários. Um exemplo seria a apresentação de propagandas publicitárias quando o usuário digita erroneamente o nome do produto ou do site. A quinta prática estaria conectada com a adoção de um trabalho forçado, isto é, o consumidor é obrigado a esperar um tempo ou são inseridas perguntas adicionais para que determinadas ações possam ser praticadas pelos utilizadores das plataformas.

Podem ser inseridas, ainda, ações que interrompam as iniciativas tomadas pelos usuários, forçando-os a ver determinado anúncio ou apresentando elementos extremamente sensíveis na interface do site. Tais práticas são verificáveis em plataformas como o Youtube, dado que o usuário é obrigado a ver uma propaganda antes que possa iniciar o vídeo ao qual queria ter acesso.

Na listagem de Mark Leiser, apresenta-se o uso de elementos de manipulação de navegação e ofuscação, em que as informações importantes ao usuário são inseridas no final da página do site ou são dificilmente localizáveis pelos cidadãos. Também podem ser aplicadas restrições a funcionalidades que são relevantes para os consumidores, o que limita, omite ou esconde certos controles necessários para realização de alguma ação.

Por fim, fala-se em práticas de choque, nas quais o usuário se depara com um conteúdo perturbador. Além disso, apresenta-se os truques que são táticas para enganar o consumidor, como a instalação de softwares adicionais sem o consentimento do navegante ou até mesmo a inclusão de anúncios falsos[207].

Nota-se dos exemplos listados que os padrões obscuros podem ser utilizados não só para enganar como também para induzir que os consumidores adotem determinado posicionamento nas plataformas digitais. Jordyn Michaels estabelece que os *dark patterns*, entretanto, não encontram utilização apenas nos sites de vendas ou de anúncios de produtos e serviços. Nas eleições norte-americanas de 2016, foram adotadas tais práticas para compartilhamento de desinformação nas redes sociais.

O Facebook teria distribuído nos painéis dos usuários notícias eleitorais que se relacionariam com as preferências anteriores de cada um. O impulsionamento de artigos na plataforma perpassaria por uma análise prévia dos dados dos usuários, a fim de que eles só

[207]LEISER, 2022, p. 502.

tivessem contato com matérias jornalísticas que seguissem suas opiniões políticas. A veracidade das informações transmitidas também não era confirmada pela empresa, o que fez com que falsos sites de notícias fossem partilhados como verdadeiros.

A adoção pelo Facebook de uma interface que listava todos os artigos de notícias como se fossem igualmente verdadeiros fez com que os usuários da plataforma tivessem contato com diversas informações falsas. Essa prática, que pode ser caracterizada como um *dark pattern*, impactou diretamente no resultado das eleições norte-americanas do ano de 2016[208].

O uso de padrões obscuros, no entanto, não se confunde com práticas de *marketing* e propaganda realizadas pelas plataformas digitais. Lucas Sérvio Gonçalves Ramadas[209] estabelece que o *marketing* advém de estudos prévios e detalhados que buscam atrair consumidores para determinadas práticas ou produtos sem ludibriá-los ou induzi-los ao erro. Já os *dark patterns* não objetivam ressaltar qualidades ou vantagens dos bens oferecidos, mas enganar o usuário a agir de uma forma diferente da que ele próprio busca.

Essa diferenciação em relação ao *marketing* e a propaganda fizeram com que a atenção dos governantes e legisladores de vários países se voltasse para o enquadramento jurídico dos *dark patterns* como práticas a serem rechaçadas. Nos Estados Unidos da América, o governo da Califórnia realizou uma emenda à lei de consumo do estado, a fim de regulamentar as táticas de padrões obscuros.

Em 2018, foi sancionado pelo Governador da Califórnia o Código de Privacidade do Consumidor (CCPA) do Estado. Em 2019, foram editadas diversas emendas à legislação, inclusive a Proposição 24, que trata especificamente sobre a limitação do uso de padrões obscuros. Dentre as determinações, está a garantia de acessibilidade de dispositivos de *opt-out* aos consumidores, de modo que seja facilitada a possibilidade de discordância com a política de privacidade da plataforma[210].

A legislação californiana proibiu expressamente, como explica Jordyn Michaels[211], que as plataformas digitais usem linguagem confusa, requeiram que os usuários apresentem informações desnecessárias, forcem que os consumidores passem por perguntas com o intuito

---

[208]MICHAELS, 2022, p. 180.

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

[210]MICHAELS, 2022, p. 189.

[211]*Ibidem*, p. 190.

de dissuadi-los de tomar determinada ação ou obriguem que os navegantes leiam toda a política de privacidade antes de discordar com a coleta de dados feita pelo site.

Em fevereiro de 2018, seguindo a legislação californiana, o estado norte-americano de Washington também buscou regular as questões envolvendo padrões obscuros. O estado propôs uma emenda ao seu Ato de Privacidade para declarar que os *dark patterns* seriam quaisquer práticas manipuladoras que teriam efeitos substanciais na autonomia dos usuários, tomadas de decisões e/ou escolhas. Contudo, até o segundo semestre de 2024, a lei ainda não havia entrado em vigor.

Outros estados norte-americanos, como a Virginia e o Colorado, também instituíram vedações às práticas de *dark patterns* por plataformas digitais. A edição de tais disposições demonstram uma preocupação dos governantes do país com a adoção de padrões obscuros, bem como lançam luz sobre uma questão ainda pouco disseminada, como exposto anteriormente.

No Brasil, Claudia Lima Marques, Laura Schertel Mendes e Laís Bergstein explicam que há uma preocupação com a relação entre padrões obscuros e o uso de dados pessoais, o que ensejaria a aplicação da Lei nº 13.709. Para as autoras,

> O uso de dados pessoais é outra preocupação relacionada a dark patterns. A legislação de proteção de dados é recente no Brasil. A Lei 13.709 foi promulgada em agosto de 2018 e estabeleceu uma vacatio legis de dois anos. Entre outros, os direitos dos consumidores, detentores de dados pessoais, são: i) saber para que finalidade seus dados pessoais serão processados e conhecer a finalidade específica para a qual serão processados; ii) ter acesso livre e fácil aos seus dados pessoais, gratuitamente; iii) poder fazer correções aos dados pessoais se estiverem errados ou desatualizados e até mesmo exigir que sejam apagados, se necessário; iv) não ter seus dados pessoais utilizados para fins discriminatórios, ilícitos ou abusivos; e v) ter segurança no tratamento de seus dados pessoais, para que não sejam acessados por aqueles que não estão autorizados. Entretanto, apesar dos esforços da autoridade de proteção de dados pessoais, da Autoridade Nacional de Proteção de Dados (ANPD) e do Sistema de Proteção ao Consumidor, a coleta e o uso indevido de dados pessoais, incluindo Dark patterns em Pedidos de Consentimento de Biscoitos são uma realidade difundida no Brasil. O uso extensivo de dados pessoais em contratos de marketing e de consumo é um aspecto fundamental da pesquisa sobre padrões comerciais obscuros[212].

Elas apresentam certa preocupação com a introdução de técnicas de *harvesting* ou *web scraping* (coleta na internet), caracterizadas por uma disseminação na busca por informações de uma pessoa específica ou de um determinado grupo em uma plataforma digital. Essas ações indicariam a necessidade de uma atuação das autoridades competentes, especialmente a

[212]MARQUES; MENDES; BERGSTEIN, 2023, p. 298.

ANPD, para apurar se os mencionados dados foram adquiridos por meio de um episódio de vazamento, foram fornecidos pelos titulares ou reverberam em informações públicas.

De qualquer modo, haveria a possibilidade de enquadramento das práticas de padrões obscuros como transgressões às disposições contidas no Código Brasileiro de Defesa do Consumidor. O artigo 39 da mencionada legislação estabelece uma série de práticas comerciais que seriam enquadradas como desleais, tais como a recusa a cumprir as determinações do consumidor, o envio de produtos e serviços sem a anuência do usuário, o aproveitamento da ignorância ou fraqueza dos consumidores para oferecimento de bens e a exigência de vantagens excessivas[213].

Apesar da possibilidade de aplicação das legislações correlatas, não há no ordenamento jurídico brasileiro, ainda, uma normatização expressa sobre as questões que envolvam *dark patterns*. Essa ausência de regulamentação específica não impede, como aponta Lucas Sérvio Gonçalves Ramadas[214], que o Conselho de Autorregulação Publicitária (Conar) atribua uma abusividade aos padrões obscuros.

A experiência europeia também impacta diretamente na popularização dos padrões obscuros, como na necessidade de regulamentação da matéria. Com isso, dada a importância das diretrizes estabelecidas pela GDPR para o Brasil e o resto do mundo, dedicar-se-á adiante uma análise específica sobre o Guia nº 3/2022 da EDPB.

3.1.2 *Análise do Guia nº 3/2022 da EDPB quanto aos dark patterns*

Em 2020, foi elaborado pelo *European Data Protection Board* (EDPB) um guia orientativo, ou como é nominalmente denominado "Diretrizes nº 3/2022", cujo objetivo é a orientação para o reconhecimento e a evitação de padrões obscuros em interfaces de plataformas de mídia social que violem as determinações do GDPR. No entanto, de antemão, o documento esclarece que os casos nele descritos não são exaustivos, sendo apenas uma explicação sobre possibilidades mais corriqueiras, haja vista a infinidade de situações que

[213] *Ibidem*, p. 298.
[214] RAMADAS, 2023, p. 29.

podem ser consideradas do tipo, restando aos provedores de mídias sociais a obrigação de adequar suas plataformas com o GDPR[215].

As diretrizes em questão conceituam os padrões obscuros como "interfaces e experiências de usuário implementadas em plataformas de mídia social que levam os usuários a tomar decisões não intencionais, involuntárias e potencialmente prejudiciais em relação ao processamento de seus dados pessoais"[216]. Para elas, os padrões obscuros objetivam interferir na tomada de decisão dos usuários e podem reduzir sua capacidade de proteger seus dados pessoais e realizar escolhas conscientes, sendo uma incumbência das autoridades de proteção de dados o sancionamento do uso de padrões obscuros quando eles violam os dispositivos do GDPR[217].

Os padrões obscuros abordados nas Diretrizes são, em seu relatório, divididos nas seguintes categorias:

TABELA I - Categorias de padrões obscuros para a EDPB[218]

Overloading	Na tradução, "sobrecarga", ocorre quando o usuário recebe um alto quantitativo de solicitações, informações, opções ou possibilidades, cujo objetivo é fazer com que eles compartilhem cada vez mais dados ou permitam de forma involuntária o processamento de seus dados. Nessa categoria, inserem-se três tipos de padrões obscuros: (i) *Continuous prompting*, (ii) *Privacy Maze* e (iii) *Too Many Options*.
Skipping	Na tradução, "ignorar", projeta a interface de modo a moldar a experiência dos usuários, de tal forma que eles se esquecem ou não pensam em todos os aspectos da proteção de dados. Nessa categoria, inserem-se dois tipos de padrões obscuros: (i) *Deceptive Snugness* e (ii) *Look over there*.

[215]THE EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them".** Version 2.0. Adopted on 14 February 2023. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en. 2023, p. 3.
[216]*Ibidem*, p. 3.
[217]*Ibidem*, p. 3.
[218]THE EUROPEAN DATA PROTECTION BOARD, 2023, p. 3-4.

Stirring	Na tradução, “agitação", afeta a escolha que os usuários fariam apelando para suas emoções ou usando estímulos visuais. Nessa categoria, inserem-se dois tipos de padrões obscuros: (i) *Emotional Steering* e (ii) *Hidden in plain sight.*
Hindering	Na tradução, “dificultar”, realiza a obstrução ou bloqueio do usuário em seu processo de se informar ou gerenciar os seus dados, tornando a ação difícil ou impossível de ser realizada. Nessa categoria, há três tipos de padrões obscuros: (i) *Dead end*, (ii) *Longer than necessary* e (iii) *Misleading information*.
Fickle	Na tradução, “inconstante”, significa que o design da interface é inconsistente e opaco, dificultando a navegação pelo usuário nas diferentes ferramentas de controle e proteção de dados, além de dificultar a compreensão quanto à finalidade do processamento. Nessa categoria, há dois tipos de padrões obscuros: (i) *Lacking hierachy* e (ii) *Decontextualising.*
Left in the dark	Na tradução, “deixado no escuro”, significa que uma interface foi desenvolvida de modo a ocultar informações ou ferramentas de controle de proteção de dados, além de deixar seus usuários inseguros quanto à forma como os seus dados são processados e que tipo de controle eles podem ter sobre eles em relação ao exercício de seus direitos. Nessa categoria, há três tipos de padrões obscuros: (i) *Language discontinuity*, (ii) *Conflicting information* e (iii) *Ambiguous wording of information.*

Com base na classificação acima, o EDPB apresentou uma exemplificação de cada uma das condutas. Em relação à tática de deixar no escuro, a plataforma digital pode, ao minutar a política de privacidade do site, realçar apenas as vantagens do compartilhamento de

dados. Isso faz com que os titulares entendam que inexistem riscos no fornecimento de suas informações pessoais, enganando-os para que acatem as determinações dos controladores[219].

No que se refere ao *fickle*, pode ocorrer da plataforma digital apresentar uma política de privacidade extremamente longa ou em linguagem estrangeira, o que dificulta com que o usuário efetivamente obtenha acesso a todas as informações necessárias. Já em práticas de *Left in the Dark*, a apresentação da forma de processamento de dados é feita de modo vago e impreciso. São usadas frases como "seus dados podem ser usados para aprimorar os nossos serviços" ou "você pode conferir parte das suas informações em sua conta ou analisando o que você posta em nossa plataforma"[220].

Sobre a tática de *overloading*, o EDPB estabelece como exemplo a introdução pela plataforma digital de um documento denominado como "dispositivo útil" em que são estabelecidas informações sobre práticas de privacidade e proteção de dados. Entretanto, a política de privacidade não apresenta nenhum link ou dado útil, indicando que o consumidor deverá procurar no site outras documentações a fim de deter as importantes informações sobre o uso de seus dados pessoais[221].

Para o *skipping*, o usuário, ao clicar em um botão de deletar a conta, é apresentado com a opção de *download* de suas informações pessoais, antes do encerramento da subscrição. Ao realizar as ações relacionadas ao resgate de seus dados, não é apresentada mais a página de cancelamento da conta, o que faz com que o consumidor tenha que iniciar o processamento diversas vezes[222].

O relatório estabelece que os padrões obscuros podem ser classificados em, ao menos, três categorias diferentes: efeitos no comportamento dos usuários, conteúdo utilizado e padrões de interface. O segundo trata sobre o conteúdo dos *dark patterns* veiculados, como, por exemplo, o uso de frases ou informações enganosas. Já o terceiro se conecta com a forma de apresentação da ideia em si.

Os padrões obscuros não são encontrados unicamente nas redes sociais. Há a aplicação de tais práticas em sites, políticas de cookies, videogames, aplicativos de celulares, dentre outros[223]. Por isso mesmo, o EDPB estabeleceu os princípios básicos previstos na GDPR que

[219]THE EUROPEAN DATA PROTECTION BOARD, 2023, p. 27.
[220]*Ibidem,* p. 28.
[221]*Ibidem,* p. 31.
[222]THE EUROPEAN DATA PROTECTION BOARD, 2023, p. 61.
[223]*Ibidem,* p. 11.

seriam aplicáveis às plataformas digitais que operam no país. O artigo 5º do mencionado normativo prevê que o manuseamento de dados pessoais deve ser realizado de forma justa, isto é, sem discriminação, enganação ou nocividade[224].

Se a interface da plataforma digital apresenta informações insuficientes ou enganosas, há uma clara violação às previsões do artigo 5º do GDPR, dado que não há um manuseio justo dos dados pessoais. Fora isso, a referida legislação estabelece, em seu artigo 25, que o processamento de informações pessoais deve observar os princípios da responsabilização, transparência e aplicação de ferramentas de privacidade na concepção das ferramentas (*privacy by design*).

O EDPB prevê que, no que se trata de ferramentas de *privacy by design*, a análise dos padrões obscuros deve perpassar pela ideia dos seguintes conceitos:

TABELA II - Conceitos atinentes à análise dos padrões obscuros[225]

Autonomia	Devem ser fornecidos aos titulares de dados os mais altos padrões de autonomia possíveis para determinação do uso de informações pessoais, bem como autonomia sobre o escopo e condições de uso ou processamento.
Interação	Os titulares de dados devem ser capazes de comunicar e exercer os seus direitos durante o processamento de dados feito pelo controlador.
Expectativas	O processamento de dados deve guardar relação com as razoáveis expectativas dos titulares de dados.
Escolha do consumidor	Os controladores não devem tratar os titulares de dados de forma injusta. Quando um processamento de dados pessoais é feito por propriedade de um controlador, pode-se criar uma situação de dificuldade do consumidor de cancelar o serviço, o que não é justo. Se isso for feito, haverá uma violação à possibilidade de exercício de direitos pelo titular de dados pessoais, de acordo com o

[224] *Ibidem,* p. 11.
[225] *Ibidem*, p. 13-14.

	artigo 20 da GDPR.
Balanceamento de poder	O balanceamento de poder deve ser um objetivo chave para o controlador de dados pessoais em sua relação com os titulares. Qualquer desbalanceamento de poder deve ser evitado. Quando não é possível, a ausência de igualdade deve ser reconhecida e deve ser combatida com contramedidas.
Sem mentiras	O processamento de dados pessoais deve ser feito de forma objetiva e neutra, evitando-se manipulações e enganações nas linguagens e/ou no design.
Verdade	Os controladores de dados pessoais devem disponibilizar informações sobre como o processamento de dados pessoais é realizado, seguindo estritamente o declarado, sem informações enganosas.

Com base em tais previsões, o relatório apresenta um guia de boas práticas que devem ser adotadas pelas plataformas digitais, com o intuito de enquadrá-las nas previsões contidas na GDPR para limitação dos padrões obscuros. Em primeiro lugar, é importante que sejam inseridos atalhos na interface do site para que os usuários possam facilmente acessar informações sobre o processamento de dados pessoais. Isso aprimora a experiência do consumidor, evitando práticas que visem enganá-lo ou manipular o seu comportamento[226].

Em segundo lugar, as plataformas digitais devem inserir em uma mesma aba todas as opções relacionáveis, o que facilita com que os usuários possam realizar modificações sobre as práticas que afetem sua privacidade. Todos os dados de contato do controlador ou da empresa gestora devem estar listados de forma clara na política de privacidade também[227].

Não se afasta a necessidade de disponibilização de informações sobre a Autoridade de Proteção de Dados Pessoais do país e de um link para que possam ser feitas reclamações diretas aos órgãos competentes. A apresentação de um resumo da política de privacidade adotada, o uso de linguagem simples e a utilização de exemplos são importantes para confirmar o entendimento do usuário sobre a política proposta.

[226]THE EUROPEAN DATA PROTECTION BOARD, 2023, p. 73.
[227]*Ibidem*, p. 73.

Como boas práticas, as plataformas digitais podem e devem explicar as consequências do fornecimento de dados pessoais pelos usuários, bem como trazer um contexto para as práticas adotadas pela empresa. Podem ser adotados guias que facilitem o entendimento dos consumidores sobre os seus direitos e sobre a possibilidade de consentimento ou não para o tratamento de informações pessoais.

É importante esclarecer que, no corpo das Diretrizes nº 3/2022, o EDPB estabeleceu que as disposições contidas na GDPR deveriam ser observadas com ainda mais cautela em relação aos grupos vulneráveis. Os idosos, as crianças, os portadores de deficiências visuais e os cidadãos com pouco acesso à tecnologia apresentam mais dificuldades do que a população comum para identificação das práticas de padrões obscuros instituídas pelas plataformas digitais[228].

Esse cenário fez com que a GDPR instituísse a necessidade de observação de outras limitações às plataformas digitais, levando em consideração a utilização das ferramentas pelos grupos vulneráveis. No que se refere às crianças, por exemplo, o Considerando 58 do Regulamento prevê que os dados direcionados a este grupo social devem ser redigidos de forma simples e de acordo com suas limitações etárias[229].

Apesar dos esforços lançados pelo EDPB com a edição das Diretrizes nº 3/2022, em 2022, a Organização Europeia de Consumidores (BEUC) lançou um guia de recomendações para reforma e cumprimento das disposições normativas que vedam a adoção de padrões obscuros pelas plataformas digitais. Embora o documento se baseie em uma visão consumerista do tema, as disposições listadas se aplicam também para o contexto de proteção de dados pessoais.

De acordo com o Guia de Recomendações produzido pela BEUC, as legislações europeias deveriam ser aplicadas com maior efetividade em relação às práticas de *dark patterns*. Em primeiro lugar, a organização estabelece que devem ser aplicadas sanções mais efetivas, a fim de reduzir a utilização de táticas dissuasivas e injustas por plataformas digitais[230]. Também seria importante que a efetividade das penalidades fosse confirmada por meio da realização de eventos com organizações consumeristas e com a sociedade em geral.

---

[228] *Ibidem*, p. 10.

[229] *Ibidem*, p. 11.

[230] BEUC (The European Consumer Organisation). ***"Dark Patterns" and the EU Consumer Law Acquis.*** Recommendations for better enforcement and reform. Ref: BEUC-X-2022-013 - 07/02/2022. Disponível em: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf. Acesso em: 01 set. 2024. 2022, p. 12.

Em segundo lugar, seria importante que fossem conduzidas investigações para identificar as empresas que adotam padrões obscuros, dando enfoque diretamente para setores específicos da economia. Também seria importante que as autoridades buscassem identificar os verdadeiros impactos dos *dark patterns* na utilização de plataformas digitais pelos usuários. Tais ações seriam capazes de contemplar como cada uma das táticas podem causar diferentes reações em clientes diferentes. Por exemplo, as táticas enganosas empregadas por companhias que atuam no setor de cosméticos são diferentes daquelas praticadas pelo setor alimentício[231].

Em infrações que possam ensejar o ajuizamento de uma ação judicial, as autoridades competentes devem requerer que sejam produzidos elementos probatórios básicos, com o objetivo de estabelecer quais são os padrões obscuros adotados pelos infratores e como tais ações impactam nas escolhas dos consumidores. Fora isso, os casos de *dark patterns* devem ser publicizados e as empresas devem ser compelidas a cumprirem as disposições legais sobre o tema[232].

Uma forma listada pelo guia para compelir as empresas a não adotarem padrões obscuros seria a edição de guias que expliquem como as companhias devem agir em relação à temática. Ademais, a legislação europeia deveria ser atualizada para abarcar efetivamente as questões atinentes aos *dark patterns*, especialmente no que se refere à adoção de um denominado princípio de "justiça por design". Melhor dizendo, a interface, as práticas comerciais e as comunicações aos consumidores deveriam levar em consideração o princípio da não discriminação[233].

As disposições contidas no Guia de Recomendações da BEUC demonstram que, embora existam esforços por parte das autoridades europeias para redução da utilização de padrões obscuros pelas plataformas digitais, ainda há um número expressivo de ocorrências nesse sentido. De acordo com a mencionada documentação, 11.000 sites europeus utilizam interfaces que diminuem o poder de decisão do usuário ou estabelecem obrigações sem a aceitação do consumidor[234].

Inge Graef, ao realizar um estudo do sistema regulatório europeu aplicável aos padrões obscuros, apresentou algumas proposições que seriam capazes de garantir maior efetividade na dissuasão de tais condutas. A Lei do Consumidor europeia seria aplicável à sistemática dos

---

[231] *Ibidem*, p. 12.
[232] *Ibidem*, p. 13.
[233] BEUC, 2022, p. 14.
[234] *Ibidem*, p. 4.

dark patterns por meio de princípios amplos e da boa-fé objetiva (*fairness*). A referida legislação estabeleceria que, em relação à aquisição de bens e contratação de serviços, deveria ocorrer a devolução de valores arcados pelos consumidores em virtude de opções padronizadas. Ademais, as plataformas digitais estariam compelidas a fornecerem aos usuários informações relevantes de forma direta e facilmente acessível[235].

Apesar disso, o autor estabelece que as mencionadas previsões legais teriam aplicação restrita, dado que nem sempre os padrões obscuros estariam relacionados a contratos a serem firmados com os usuários. Desse modo, a Lei do Consumidor europeia não seria aplicável diretamente em todos os casos, o que faria com que fosse necessária uma análise com base no princípio da boa-fé para que se estabelecesse se determinada prática estaria vedada ou não[236].

A outra legislação que faria parte do arcabouço regulatório europeu que enfrentaria os padrões obscuros seria a GDPR. O princípio do processamento de dados de forma não discriminatória seria utilizado como um “guarda-chuva" para proteção dos titulares de dados pessoais em face de prática de *dark patterns*, independente da possibilidade de aplicação de outros preceitos. Apesar disso, os lemas de responsabilização, transparência e *privacy by design* também seriam relevantes para o tema[237].

A Lei sobre os Serviços Digitais, promulgada em 2022, determinaria expressamente que as plataformas on-line não poderiam criar, organizar ou operar suas interfaces de forma a enganar ou manipular os usuários, reduzindo a habilidade de tomadas de decisões livres e informadas. Ainda que não seja uma vedação expressa aos padrões obscuros, a disposição normativa apresenta uma redação mais clara, o que contribui para garantir uma maior efetividade à lei[238].

Inge Graef cita, ainda, que a legislação europeia de defesa da concorrência teria um impacto significativo na vedação de padrões obscuros que causassem impactos na livre funcionalidade do mercado econômico. Essas previsões teriam um escopo mais amplo, diferente das legislações consumeristas - aplicadas individualmente - e das disposições sobre proteção de dados - aplicadas apenas às ações que envolvam tratamento de dados pessoais.

---

[235]GRAEF, Inge. The EU regulatory patchwork for dark patterns: an illustration of an inframarginal revolution in European law?. In: Toward an Inframarginal Revolution: Markets as Wealth Distributors. Cambridge University Press. 2023, p. 7.

[236]*Ibidem*, 2023, p. 7.

[237]GRAEF, 2023, p. 9.

[238]*Ibidem*, p. 10.

Os *dark patterns* poderiam ser enquadrados como táticas que garantiriam um abuso de domínio, o que restaria vedado.

A existência de um amplo arcabouço regulatório que se aplica à temática de padrões obscuros na Europa pode ocasionar um conflito de normas, uma vez que certas legislações estabelecem obrigações mais ou menos rígidas para as práticas. Esse cenário pode diminuir a efetividade das proposições, causando prejuízos para os cidadãos.

Além disso, Inge Graef esclarece que as respectivas normas preveem que a proteção contra *dark patterns* não é feita com base nos danos causados por tais ações, mas sim pelo escopo de incidência legal. Desse modo, por exemplo, a GDPR só pode ser aplicada se a plataforma digital que estiver adotando padrões obscuros também realizar o tratamento de dados pessoais[239]. Assim, podem existir práticas que não se encaixem em nenhuma das legislações existentes na Europa ou, como citado acima, que possam ser vedadas por várias normas.

A fragmentação do sistema regulatório europeu no que se refere aos padrões obscuros enseja riscos relevantes, de modo que se mostraria pertinente a edição de um regime específico para conter os malefícios causados por tais práticas. Seria importante que fossem adotadas ações coordenadas e uma política comunitária que clarifique a aplicação de cada um dos arcabouços normativos aplicáveis[240].

Levando em consideração as análises realizadas por Inge Graef, é possível perceber que, ainda que as legislações europeias, especialmente as Diretrizes nº 3/2022 da EDPB, contribuam para a regulamentação dos padrões obscuros, há um longo caminho a ser percorrido para efetiva proteção dos consumidores. A quantidade de plataformas digitais que praticam tais ações enfatizam que as documentações não foram capazes de efetivamente inibir essas táticas.

Entretanto, é impossível afastar os benefícios que uma sistematização e uma proteção regulatória podem ensejar aos cidadãos. A preocupação, além da difusão dos direitos dos usuários, é na própria ausência de ciência por parte de grande parte do público sobre os padrões obscuros. Com isso, a apresentação de recomendações e a realização de workshops podem ser importantes passos para diminuição dos malefícios causados por eles.

---

[239] *Ibidem*, p. 18.
[240] GRAEF, 2023, p. 20.

Por fim, é importante estabelecer que as disposições contidas nas Diretrizes nº 3/2022 se aplicam a um contexto de tratamento de dados pessoais, o que significa que há um escopo restrito para vedação de tais práticas. Desse modo, estabelece-se a necessidade de visualização da temática por padrões mais gerais e por princípios que possam ser aplicáveis não só ao âmbito da proteção aos titulares de informações pessoais como também em outras sistemáticas.

No próximo tópico será tratado sobre a correlação entre padrões obscuros e violação à boa-fé objetiva (*fairness*), o que perpassa por uma ótica mais genérica sobre a necessidade de proteção dos usuários de plataformas digitais em relação a práticas que visem enganá-los ou que reduzam significativamente o seu poder de decisão.

3.1.3 *Padrões obscuros e violação à boa-fé objetiva (fairness)*

O princípio da boa-fé objetiva apresenta um papel fundamental no Direito do Consumidor e no Direito Privado em sentido amplo. O preceito encontra respaldo expresso no art. 4º, III, do Código de Defesa do Consumidor Brasileiro, que o consagra como uma espécie de guia para a análise das relações jurídicas estabelecidas entre fornecedores e consumidores. Quanto a isso, a literatura estabelece que a análise sobre o princípio da boa-fé passa por um enfrentamento das diferenças existentes entre as noções de objetividade e subjetividade que envolvem o conceito. A boa-fé subjetiva não pode ser classificada como um preceito jurídico, dado que se insere no âmbito do estado psicológico de determinado cidadão e que se torna requisito necessário para a aplicação de determinadas legislações. Nesse cenário, a subjetividade trata sobre a inexistência de conhecimento por parte do envolvido acerca de alguma situação jurídica ou a ausência de interesse na produção de algum resultado danoso em relação a outrem[241].

No que se refere à boa-fé objetiva, Miragem[242] explica que há a observação de um princípio jurídico em si. Tal preceito exige que, nas relações firmadas entre consumidores e fornecedores, haja uma espécie de lealdade e respeito de uns para com os outros, implicando com que as partes ajam de uma forma legítima e correta. Portanto, nota-se que o princípio da

[241]MIRAGEM, Bruno. **Curso de Direito do Consumidor**. 9. ed. Rio de Janeiro: Editora Forense, 2024, p. 114.
[242]*Ibidem*, p. 114.

boa-fé objetiva desempenha um papel fundamental na harmonização dos interesses envolvidos tanto nas relações consumeristas quanto nas civis em geral.

Segundo Luiz Antônio Rizzato Nunes[243], o princípio, presente no artigo 4º do CDC, busca compatibilizar interesses que, à primeira vista, podem parecer conflitantes, como a proteção do consumidor e o desenvolvimento econômico e tecnológico. Desse modo, a boa-fé objetiva não se limita à defesa do lado mais frágil da relação, mas também orienta a interpretação jurídica em consonância com os princípios constitucionais que fundamentam a ordem econômica, especialmente a harmonia estabelecida pelo artigo 170 da Constituição Federal.

Além disso, o princípio da boa-fé objetiva vai além de sua função em relações específicas, pois exerce influência significativa na construção do próprio sistema jurídico brasileiro. Ele tem um papel crucial na aplicação prática de outros princípios e normas jurídicas que sustentam o modelo de sociedade capitalista contemporânea. Esse princípio, inserido no contexto linguístico dos operadores do direito e erigido como princípio na Lei nº 8.078/1990 (CDC), foi posteriormente adotado pelo Código Civil de 2002, ganhando reconhecimento como um dos elementos centrais do sistema jurídico constitucional brasileiro[244].

A boa-fé, até o ano de 1990, era aplicada pelas Cortes Brasileiras, essencialmente, em sua acepção subjetiva. O Código Civil de 1916, por exemplo, previa que o termo estava relacionado somente com a ausência de ardil ou de consciência por parte do cidadão de que determinada situação estaria relacionada a uma transgressão legal. Dessa forma, a visão sobre o estado psicológico do envolvido interligava-se diretamente ao que se compreendia como boa-fé. Com a evolução do capitalismo e desenvolvimento de uma cultura de massas, observou-se a necessidade de proteção de parcelas da população que se encontravam em uma situação mais fragilizada frente aos abusos dos grandes agentes econômicos. Assim, foi promulgado o Código de Defesa do Consumidor no Brasil, em setembro de 1990[245].

A lei, como já abordado, inaugurou a acepção de boa-fé objetiva no país. Na realidade, a noção de boa-fé como um preceito jurídico surgiu no direito alemão, mais especificamente

---

[243]NUNES, Luiz Antônio Rizzato. **Comentários ao código de defesa do consumidor**. In: Minha Biblioteca, (8th edição). Grupo GEN, 2015, p. 77.

[244]*Ibidem*, p. 77

[245]TEPEDINO, Gustavo; SCHREIBER, Anderson. Os efeitos da Constituição em relação à Cláusula da Boa-fé no Código de Defesa do Consumidor e no Código Civil. **Revista da EMERJ**, v. 6, n. 23, Rio de Janeiro, 2003, p. 139.

no parágrafo 242 do Código Civil de 1900 (BGB). A referida legislação estrangeira previa que os contratantes deveriam sempre agir em observância à boa-fé e às utilizações do tráfico[246]. Tal disposição, assim como estabelecido no nosso Código de Defesa do Consumidor, deve ser observada igualmente por ambas as partes envolvidas em determinada relação jurídica, não sendo uma norma protetiva apenas dos consumidores[247].

Posteriormente, com a edição do Código Civil de 2002, passou-se a prever a aplicação da boa-fé objetiva também às relações contratuais. O art. 422 da referida norma estabelece que "Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé"[248]. Nesses termos, Tepedino e Schreiber alertam que a visão que se objetivou adotar no âmbito cível foi a mesma conferida pela lei consumerista[249].

A boa-fé no contexto cível teria uma tríplice aplicação. Isto é, a garantia de uma função interpretativa aos instrumentos firmados com base no Código Civil, a objetividade de criação de deveres acessórios às obrigações principais, além da restrição a determinados abusos contratuais. Há, então, o estabelecimento de uma visão hermenêutica e de um desenvolvimento de obrigações e de formas de agir[250].

O princípio da boa-fé objetiva desempenha um papel transformador na compreensão das relações obrigacionais, segundo Bruno Miragem[251]. Esse princípio estabelece que as obrigações contratuais devem ser entendidas como dinâmicas, abarcando todas as fases da relação jurídica, desde o surgimento da obrigação até seu cumprimento e, eventualmente, até mesmo após a extinção do contrato.

Dessa forma, há a exigência de que as partes ajam de maneira leal e honesta em todos os momentos: ao firmar o contrato, durante sua execução e, se necessário, no período posterior ao seu encerramento. Antes da celebração do contrato, deve-se fornecer informações claras e corretas, garantindo transparência e compreensão para todos os envolvidos; durante a execução, há a necessidade de observância dos deveres estabelecidos pelo próprio objeto do

[246]MIRAGEM, 2024, p. 114.
[247]TEPEDINO; SCHREIBER, *op. cit.*, p. 142.
[248]BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 20 mai. 2023. Acesso em: 01 set. 2024. (n. p.)
[249]TEPEDINO; SCHREIBER, 2003, p. 143.
[250]*Ibidem*, p. 144.
[251]MIRAGEM, 2024, p. 114.

contrato; e, após sua extinção, alguns deveres podem ainda subsistir, como a responsabilidade por eventuais vícios ocultos[252].

Além disso, o princípio da boa-fé objetiva leva ao surgimento de deveres acessórios ou laterais, que vão além das obrigações principais estabelecidas pelo contrato, como o pagamento de um preço ou a entrega de um bem. Esses deveres complementares servem para assegurar que os interesses globais das partes sejam respeitados e incluem responsabilidades como prestar cuidado, promover a segurança, cooperar mutuamente, fornecer informações precisas e proteger tanto o patrimônio quanto a integridade pessoal das partes envolvidas. Esses deveres laterais reforçam a necessidade de uma atuação que vá além do simples cumprimento do contrato, buscando um comportamento ético e alinhado aos princípios da confiança e da boa-fé em toda a relação jurídica[253].

No campo do direito do consumidor, a boa-fé objetiva manifesta-se de forma particularmente importante. Nos contratos de consumo, por exemplo, os fornecedores são vinculados por suas ofertas e pela publicidade que veiculam, gerando uma expectativa legítima nos consumidores. Além disso, o CDC, em seu artigo 46, prevê a nulidade de contratos que não forneçam ao consumidor a oportunidade de conhecer seu conteúdo previamente ou que sejam redigidos de maneira a dificultar a compreensão do seu significado. Desse modo, o princípio da boa-fé objetiva funciona como um mecanismo de proteção do consumidor, assegurando que os contratos sejam claros, justos e transparentes, e que os interesses de todas as partes sejam adequadamente considerados e respeitados[254].

A criação de deveres anexos não pode ser interpretada como de incidência ilimitada. Por exemplo, com base na boa-fé objetiva, um vendedor de carros deve informar aos seus clientes todas as informações que sejam necessárias para efetivamente garantir a escolha livre e segura sobre a compra do veículo ou não. Entretanto, o dever de informação, obrigação acessória advinda do princípio da boa-fé objetiva, não obriga com que o pracista apresente dados sobre sua vida privada ou opiniões pessoais[255].

De modo a contextualizar as figuras parcelares à boa-fé objetiva, pode-se listar o *venire contra factum proprium*, a *supressio*, a *surrectio* e a *tu quoque.* A figura do *venire contra factum proprium*, conhecida como teoria dos atos próprios, veda o comportamento

[252]*Ibidem*, p. 114.
[253]*Ibidem*, p. 114.
[254]*Ibidem*, p. 114.
[255]TEPEDINO; SCHREIBER, 2003, p. 146.

contraditório. Isso ocorre quando uma parte, após adotar uma determinada conduta ou omitir-se, surpreende a contraparte com um comportamento oposto, quebrando a confiança estabelecida. Observa-se que, se legitimada, essa contradição pode culminar em abuso de direito. Assim, essa figura é essencial para proteger expectativas legítimas e evitar que o exercício de um direito prejudique a confiança anteriormente gerada[256].

Já as figuras da *supressio* e *da surrectio* estão diretamente relacionadas ao fator tempo e à reiteração de comportamentos. Na *supressio*, há a perda de um direito pelo não exercício em tempo razoável, gerando a expectativa de que ele não será mais exigido. Um exemplo está no artigo 330 do Código Civil, que trata da renúncia tácita de um credor ao aceitar reiteradamente o pagamento em local diverso do acordo[257]. Por outro lado, a *surrectio* refere-se ao surgimento de um novo direito em razão da prática continuada de determinados atos, criando uma obrigação subjetiva. Ambas visam garantir a estabilidade das relações obrigacionais frente a alterações de conduta ao longo do tempo[258].

Há ainda a vedação de exigência de direitos que não se possui, conforme o princípio de que não se pode beneficiar da própria torpeza (*tu quoque*). Inspirada no significado histórico de traição, essa figura reforça os valores de isonomia e boa-fé contratual, combatendo o abuso de direito e promovendo o equilíbrio nas relações jurídicas[259]. Juntas, essas figuras parcelares da boa-fé demonstram objetivamente a complexidade e a relevância desse princípio, cuja aplicação transcende as situações descritas, ocorrendo como instrumento de justiça e equidade em diversas áreas do Direito.

A Lei Geral de Proteção de Dados brasileira também prevê, em seu artigo 6º, a necessidade de observância da boa-fé em todos os tratamentos de dados realizados no país. Bruno Bioni explica que os princípios da boa-fé e a confiança dos titulares estão intrinsecamente interligados no âmbito da referida legislação. Tais preceitos se coadunam com a necessidade de aceitação e internalização de condutas corretas e adequadas por parte dos envolvidos nas atividades que manuseiam informações pessoais[260].

A boa-fé estabelecida pela LGPD é a acepção objetiva do termo, como abordado na obra Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro. O

---

[256] PENTEADO, Luciano de Camargo. Figuras parcelares da boa-fé objetiva e venire contra factum proprium. **Revista de direito privado**, v. 27, n. 1, p. 252-278, 2006. p. 51.
[257] *Ibidem*. p. 59.
[258] *Ibidem.* p. 60.
[259] *Ibidem. p. 54.*
[260]BIONI, 2021, p. 234.

dever de informação previsto no mencionado normativo, por exemplo, realiza um paralelo direto com o princípio da boa-fé, dado que há a necessidade de correto fornecimento de dados para que o titular possa tomar uma decisão sobre a necessidade de consentimento ou não[261] (Frazão, Tepedino, Oliva, 2020).

Até mesmo para o tratamento de informações públicas, a LGPD prevê, no seu artigo 7º, § 3º, que há a necessidade de observância da boa-fé. Esse cenário demonstra o importante papel que o princípio adquire para a proteção de informações pessoais, sendo uma espécie de fonte equilibradora das exigências feitas aos agentes de tratamento sobre a necessidade de proteção da segurança e sigilo[262].

A preocupação do legislador em estabelecer a boa-fé como um princípio para regulação do tratamento de dados pessoais no Brasil advém do cenário atual vivenciado no país. Há uma grande desigualdade entre as informações fornecidas aos cidadãos e aquelas de conhecimento dos operadores de dados pessoais. As grandes companhias e o Governo em si apresentam maiores poderes, recursos e dados sobre as principais relações instituídas entre esses agentes e a população[263].

Dessa forma, no âmbito da proteção de dados pessoais, o princípio da boa-fé assume a mesma visão objetiva já consagrada pelo Código Civil e pelo Código de Defesa do Consumidor. Nesse formato, como estabelecido acima, há uma necessidade de aplicação das três funções da boa-fé objetiva no âmbito dos tratamentos de informações pessoais, de modo que tal preceito assume as funções de integração, interpretação e controle.

Quanto à experiência internacional, a Organização Europeia de Consumidores (BEUC) lançou um importante projeto sobre a aplicação da boa-fé objetiva (*fairness*) aos consumidores digitais. A organização parte de uma visão de vulnerabilidade digital para explicar como, na sociedade atual, há uma alteração na dinâmica das relações. Não é possível estabelecer que somente características fixas de um cidadão sejam capazes de provocar uma fragilidade. Em verdade, a interação com o ambiente virtual pode causar fraquezas momentâneas ou, até mesmo, praticáveis somente em dado contexto[264].

---

[261]FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2020, (n.p.).

[262]FRAZÃO; TEPEDINO; OLIVA, 2020, (n.p.).

[263]*Ibidem*.

[264]BEUC (The European Consumer Organisation). **"Digital Fairness for Consumers"**. Natali Helberger, Betül Kas, Hans-W. Micklitz, Monika Namysłowska, Laurens Naudts, Peter Rott, Marijn Sax, Michael

Nos textos estrangeiros, inclusive na publicação realizada pela Organização Europeia de Consumidores, utiliza-se o conceito de *fairness* para tratar sobre a proteção dos usuários frente ao ambiente digital. O conceito está interligado à ausência de execução de ações que explorem a assimetria e a vulnerabilidade de certos usuários[265]. Assim, apesar de não serem conceitos expressamente idênticos, é possível traçar um paralelo direto entre o conceito de boa-fé objetiva e *fairness*, dado que ambos se voltam para a busca do estabelecimento de uma lealdade nas relações firmadas entre diferentes partes no contexto consumerista, cível ou de proteção de dados pessoais.

Estabelecido o paralelo entre *fairness* e boa-fé objetiva, a análise do texto publicado pelo BEUC será feita com base na correlação entre esses dois institutos, uma vez que ambos parecem dispor sobre o estabelecimento de uma confiabilidade nas relações, especialmente no que se refere à troca de informações, aquisição e venda de serviços/bens no ambiente virtual.

Todos os consumidores podem ser listados como vulneráveis dependendo das circunstâncias e do contexto em que se inserem, de acordo com o BEUC. A concepção de vulnerabilidade digital envolve três conceitos básicos: natureza da relação, arquitetura referencial e a erosão da privacidade. Nessa dinâmica, é possível que a interface de uma determinada plataforma digital, aplicativo ou outra infraestrutura de rede seja capaz de culminar em uma situação vulnerável.

Desse modo, é necessário conferir uma atenção especial à relação existente entre vulnerabilidade e manipulação. O Ato de Regulação de Inteligência Artificial proposto pela União Europeia, como explica o BEUC, aborda uma nova categoria de pessoas vulneráveis que foge da primeira acepção, vinculada às legislações consumeristas. A proposta prevê que, além dos idosos, crianças e deficientes, devem ser considerados como agentes mais frágeis os imigrantes, as pessoas em situação de pobreza e as minorias religiosas e/ou étnicas. São, ainda, estabelecidos grupos populacionais que, dependendo da situação, podem ser enquadrados como indefesos[266].

Essa previsão de proposta legal se revela como um importante reconhecimento por parte da Comissão responsável pelo texto de que as características de alguns cidadãos podem

---

Veale. Brussels, March 2024. Disponível em: https://discovery.ucl.ac.uk/id/eprint/10189356/. Acesso em: 05 set. 2024. 2024, p. 11.

[265] *Ibidem*, p. 230.

[266] BEUC, 2024, p. 13.

ser usadas, indevidamente, para manipulá-los a tomarem algumas decisões e ações que não lhes sejam interessantes. Com isso, estabelece-se que a proteção dos usuários nos meios digitais deve alcançar um novo ambiente que culmine na introdução de práticas denominadas como *"digital fairness by design"*[267].

Como estabelecido no início deste capítulo, a ideia de *fairness* conecta-se diretamente com o princípio da boa-fé objetiva. Desse modo, é possível tratar a noção de *"digital fairness by design"* como uma prática correlata à aplicação da boa-fé objetiva em todos os ambientes de informação. O BEUC estabelece a *"digital fairness by design"* como sendo uma abordagem em que se manifesta uma integração do princípio da boa-fé desde o início de determinada situação jurídica. Ao invés de aguardar que ocorram ações que violariam tais preceitos, opta-se por uma adoção de medidas acautelatórias[268].

A ênfase da adoção do parâmetro de *"digital fairness by design"* é a de que não basta que a regulação simplesmente responda aos incipientes problemas que possam surgir e que manipulem os cidadãos e consumidores, tais como os *dark patterns*. A redução da aplicação de padrões obscuros só poderá ocorrer com o entendimento de que a vedação de tais táticas deve ocorrer em um formato de prevenção e antecipação de escolhas de interfaces que possam impactar a experiência dos usuários[269].

A proposição do BEUC mostra-se tão pertinente que merece ser aprofundada no tópico seguinte do presente texto. De qualquer forma, é importante estabelecer informações adicionais que são listadas pela entidade e que se relacionam diretamente com a necessidade de aplicação da boa-fé objetiva ao panorama digital do Brasil, especialmente no que se refere às práticas de padrões obscuros.

Nos termos explicados anteriormente, não existe uma definição única na doutrina para o termo *dark patterns*. Michaels[270] afirma, por exemplo, que padrões obscuros estariam conectados à aplicação de truques nas interfaces digitais para que os usuários tomem decisões que não teriam intuito, como a assinatura de algum programa. Essa concepção, por abarcar um conceito claro, pode ser aplicada ao contexto em debate.

Os padrões obscuros, então, estão diretamente ligados à manipulação para que haja um cerceamento do direito de escolha do usuário em plataformas digitais. Dessa forma, a

---

[267] *Ibidem*, p. 166.
[268] *Ibidem*, p. 166.
[269] *Ibidem*, p. 167.
[270] MICHAELS, 2022, p. 178.

aplicação da boa-fé objetiva e da visão de *"fairness"* enquadra-se diretamente na regulação da impossibilidade de continuidade de tais práticas. Há um reforço das vulnerabilidades dos consumidores para que sejam aplicadas táticas que violam não só o Código do Consumidor, como também a própria LGPD.

Esse cenário faz com que o princípio da boa-fé objetiva alcance um status importante para a redução de práticas de padrões obscuros e para proteção dos usuários, especialmente os mais vulneráveis, frente às plataformas digitais. Nesse ponto, cabe esclarecer que, conforme consignado pelo BEUC, inexiste uma fragilidade estática, de modo que as concepções do sistema impactam diretamente no entendimento sobre quais atores estariam menos protegidos.

A proteção dos indivíduos frente aos padrões obscuros envolve, então, não só uma avaliação sobre a necessidade de adoção integral da boa-fé objetiva, como também a análise sobre as possíveis vulnerabilidades existentes no sistema. Assim, reforça-se que os *dark patterns* podem representar riscos para o direito do consumidor, o direito civil e a LGPD, o que enseja a aplicação do conceito de boa-fé objetiva para proteção dos indivíduos no país.

Feitos tais esclarecimentos, buscaremos relacionar as figuras parcelares à boa-fé objetiva às espécies de *dark patterns* já listados no tópico 3.1.2, de modo a verificar a violação de forma direta. Os padrões obscuros utilizados em interfaces digitais representam práticas que violam os princípios da boa-fé objetiva e suas figuras parcelares, prejudicando a transparência, a confiança e o equilíbrio entre as partes. Um exemplo é o padrão "*Overloading*", que sobrecarrega o usuário com solicitações, informações ou opções excessivas. Essa prática viola o dever de informação ao criar um ambiente propositalmente confuso, dificultando a tomada de decisões conscientes. Subcategorias como o "*Continuous Prompting*" inundam o usuário com solicitações repetitivas, enquanto o "*Privacy Maze*" apresenta uma estrutura complexa que impossibilita a compreensão clara das opções disponíveis. Já o "*Too Many Options*" desrespeita a vedação ao comportamento contraditório, ao frustrar expectativas legítimas de clareza e simplicidade.

O padrão "*Skipping*" projeta a interface de forma a induzir o usuário a ignorar aspectos importantes da proteção de dados, infringindo o dever de lealdade e a figura da *supressio*. O "*Deceptive Snugness*" cria uma falsa sensação de segurança que mascara riscos reais, manipulando a percepção do usuário. Por sua vez, o "*Look Over There*" desvia a atenção para

informações irrelevantes, deixando de cumprir o dever de informar adequadamente e prejudicando o exercício consciente dos direitos pelo usuário.

Já o padrão "*Stirring*" explora as emoções e estímulos visuais para influenciar as escolhas dos usuários, o que configura uma violação à proibição do abuso de direito e ao dever de lealdade. Práticas como o "*Emotional Steering*" manipulam decisões com base em apelos emocionais, explorando vulnerabilidades psicológicas de forma desleal. Além disso, o "*Hidden in Plain Sight"* esconde informações importantes sob uma aparência de simplicidade ou elementos visuais distrativos, desrespeitando o dever de transparência e de fornecer informações claras.

O padrão "*Hindering*" dificulta o acesso e o gerenciamento de dados pessoais, violando o dever de cooperação e a *supressio.* O "*Dead End*" impede o usuário de concluir ações ou exercer direitos ao criar barreiras artificiais, violando tanto o dever de informação, por limitar a visibilidade do usuário, como é um *Venire contra factum proprium*. O "*Longer Than Necessary"* prolonga processos desnecessariamente, dificultando ainda mais a navegação e a compreensão configurando uma *supressio,* enquanto o "*Misleading Information*" utiliza informações imprecisas ou contraditórias, comprometendo a confiança e a lealdade que deveriam reger as relações contratuais, além de perfazer um comportamento contraditório, a tradução do *Venire contra factum proprium.*

No caso do padrão "*Fickle*", o design inconsistente e opaco das interfaces prejudica a navegação do usuário e dificulta a compreensão das finalidades de processamento de dados, violando o dever de informação e a vedação ao comportamento contraditório. A ausência de hierarquia clara nas informações, como ocorre no "*Lacking Hierarchy*", confunde os usuários e inviabiliza o cumprimento de expectativas legítimas. O "*Decontextualising*", por sua vez, apresenta informações fora de contexto, o que mina ainda mais a transparência e a confiança.

Por fim, o padrão "*Left in the Dark*" caracteriza-se pela ocultação de informações ou ferramentas de controle, deixando os usuários inseguros quanto ao tratamento de seus dados. Essa prática viola o dever de transparência e de cooperação, ao criar um ambiente de incerteza e desconfiança. A "*Language Discontinuity*" utiliza linguagem confusa ou técnica demais, dificultando a compreensão por parte dos usuários. Já o "*Conflicting Information*" fornece informações contraditórias, frustrando expectativas legítimas, enquanto o "*Ambiguous Wording of Information*" utiliza intencionalmente palavras ambíguas para evitar um entendimento claro, prejudicando o exercício dos direitos do usuário.

De modo a simplificar os enquadramentos realizados, formulamos a seguir uma tabela simples com as correlações:

TABELA III – Padrões obscuros e figuras parcelares à boa-fé objetiva

Padrão obscuro	**Subcategoria**	**Descrição**	**Figuras parcelares violadas**
Sobrecarga (*Overloading)*	Solicitação contínua (*Continuous prompting*)	Solicitações repetitivas que confundem o usuário	Dever de informação
	Labirinto de privacidade (*Privacy Maze)*	Estrutura complexa que dificulta o entendimento	Dever de Informação e Dever anexo de cooperação
	Excesso de opções *(Too Many Options)*	Múltiplas alternativas sem hierarquia clara	Vedação ao comportamento contraditório (*venire contra factum proprium*)
Ignorar (*Skipping*)	Aconchego enganoso (*Deceptive Snugness)*	Falsa sensação de segurança que mascara riscos	Dever de lealdade e *Supressio*
	Olhe ali *(Look over there*)	Desvia a atenção de aspectos importantes	Dever de informação
Agitação (*Stirring*)	Direção emocional (*Emotional Steering*)	Manipulação de escolhas por apelos emocionais	Dever de cooperação
	Escondido à vista de todos (*Hidden in Plain Sight*)	Informações ocultas por elementos visuais distrativos	Dever de transparência e Dever de informação

Dificultar *(Hindering)*	Beco sem saída *(Dead end)*	Impedir o usuário de concluir ações ou exercer direitos	Dever de cooperação e *Venire contra factum proprium*
	Mais longo que o necessário *(Longer than necessary)*	Processos desnecessariamente longos	*Supressio*
	Informações Enganosas *(Misleading information)*	Informações imprecisas ou contraditórias	Dever de lealdade, Dever de informação, Dever de transparência e *Venire contra factum proprium*
Inconstante *Fickle*	Falta de Hierarquia *(Lacking Hierarchy)*	Falta de posição que confunde a navegação	*Dever de informação*
	Descontextualizando *(Decontextualising)*	Informações fora de contexto que dificultam a compreensão	*Verire contra factum proprium*
Deixado no escuro *(Left in the Dark)*	Descontinuidade da linguagem (*Language Discontinuity*)	Linguagem excessivamente ténica ou confusa a ponto de dificultar o entendimento	Dever de transparência
	Informações conflitantes (*Conflicting Information*)	Informações contraditórias que frustram expectativas	Dever de cooperação

	Formulação ambígua *(Ambiguous Wording of Information)*	Linguagem ambígua que gera incertezas	Dever de informação

Esses padrões evidenciam como práticas de design podem infringir os pilares da boa-fé objetiva, ao criar um ambiente desleal e desequilibrado. A falta de transparência e de informações claras compromete não apenas a relação de confiança, mas também o próprio exercício dos direitos pelos usuários, perpetuando uma assimetria de poder incompatível com os princípios éticos que deveriam reger as relações contratuais.

Feitas tais correlações no âmbito da boa-fé objetiva e suas figuras parcelares, adentraremos no último tópico do trabalho, no qual nos propusemos a apresentar a estratégia de contorno aos padrões obscuros.

3.2 Estratégia de contorno aos padrões obscuros no Brasil

Como demonstrado ao longo do presente capítulo, os *dark patterns* representam um risco para os usuários de plataformas digitais, dado que impactam diretamente na prática de ações conscientes pelos consumidores, o que enseja uma redução na autonomia, na confiança e na segurança dos usuários dentro destes ecossistemas. As táticas de *dark patterns* podem ser interligadas a diversos tipos diferentes de classificações, sendo exemplos a adição de produtos em carrinhos de compras, a confirmação automática de inscrição de um consumidor em custos ocultos, a utilização de ferramentas de indicação de falsa escassez, o uso de perguntas ardilosas, dentre tantas outras[271].

A partir desse cenário, mostra-se necessária a introdução de mecanismos que sejam capazes de regular e reduzir a aplicação de padrões obscuros em ferramentas digitais. As primeiras práticas que seriam relevantes para concretização da redução do número de

[271]MARQUES; MENDES; BERGSTEIN, 2023, p. 3.

plataformas que utilizam, no Brasil, *dark patterns* podem ser resumidas na listagem realizada pelo BEUC.

Atualmente, no ordenamento jurídico brasileiro, prevê-se a possibilidade de aplicação de princípios abrangentes, como o da boa-fé objetiva, e/ou legislações correlatas para vedação das práticas de padrões obscuros por plataformas digitais. Como estabelecido no tópico anterior, as vedações às práticas que violem a lealdade das relações são punidas no âmbito cível, consumerista e de proteção de dados. Entretanto, inexiste uma resolução normativa própria e clara sobre a temática no Brasil.

Fora isso, a pulverização de informações em diversas normas diferentes que podem ser aplicadas, dependendo da análise realizada, dificulta a proteção dos usuários. Conforme pesquisa conduzida por Inge Graef, na União Europeia, a proteção contra *dark patterns* é realizada por meio do escopo de incidência normativa[272]. Isto é, se está em debate uma relação de consumo, aplica-se a legislação consumerista. De acordo com o referido autor, esse formato de regulação abre brechas para que existam práticas que não se amoldem aos padrões legislativos e possam seguir sendo aplicadas indiscriminadamente pelos aplicativos de internet.

Apesar da pesquisa conduzida ter sido feita na União Europeia, esse entendimento é ainda mais gravemente aplicável ao Brasil. O país carece de uma legislação própria ou, até mesmo, de uma disciplina correlata que trate sobre as práticas de padrões obscuros propriamente ditos. Embora seja possível o enquadramento das mencionadas ações em outros diplomas normativos, tal vedação não resta clara. Fora isso, estabelece-se a necessidade de enquadramento das ações quanto ao escopo do dano, o que, como abordado por Inge Graef, culmina no fornecimento de proteção insuficiente para os cidadãos.

Desse modo, torna-se imprescindível a edição de uma legislação sobre o tema que seja capaz, inclusive, de ser efetivamente aplicada no contexto brasileiro. Como se extrai da documentação produzida pelo BEUC, embora a União Europeia conte com um normativo claro sobre a vedação de práticas de padrões obscuros, a política regulatória nem sempre é verdadeiramente aplicada[273].

Para a edição de normativo no Brasil, seria interessante a avaliação da experiência de outros países, com o objetivo de criar uma legislação que seja efetiva e que preveja sanções

[272]GRAEF, 2023, p. 18.
[273]BEUC, 2022, p. 12.

que as autoridades sejam capazes de executar. Até que seja possível a finalização de um procedimento legislativo para a regulação do tema, são pertinentes as sugestões das autoras Claudia Lima Marques, Laura Schertel Mendes e Laís Bergstein de aplicação de medidas estruturais.

De acordo com as referidas escritoras, é possível o combate de práticas de padrões obscuros no Brasil através do processo coletivo, previsto no Código de Processo Civil brasileiro. Entretanto, tais ações apresentam uma capacidade reduzida de proteção dos direitos dos cidadãos, ante o fato de que, normalmente, são prolatadas diversas decisões genéricas que, em verdade, correspondem apenas a uma soma de posicionamentos individuais. Dessa forma, impõe-se a necessidade de envolvimento da prática de decisões estruturais, assim como ocorre na doutrina norte-americana[274].

As ações estruturais, diferente do que pode ser abordado por críticos, não violam o princípio da separação dos poderes. A autoridade judicial não serve apenas para decidir sobre o direito da parte que se socorre ao Judiciário. Em verdade, no momento de prolação de uma decisão, o juiz deve fazer do direito reconhecido uma realidade prática para todo o país. Com isso, a adoção desse tipo de prática para prevenir a ocorrência de padrões obscuros no Brasil mostra-se pertinente[275].

Ademais, as medidas estruturais encontram amparo na legislação consumerista brasileira, uma vez que há a previsão, nos artigos 83 e 84 do Código de Defesa do Consumidor, de que, para resguardar os direitos e interesses das relações estabelecidas no referido normativo, podem ser implementados todos os tipos de medidas capazes de proteger os consumidores e solucionar os eventuais danos causados[276].

As decisões estruturais têm se destacado como uma alternativa eficaz para lidar com demandas complexas que afetam coletivamente certos grupos de pessoas, promovendo a reorganização de estruturas que se encontram em desequilíbrio. Essas decisões são fundamentais quando a situação exige mais do que a simples reparação pontual de um direito violado, buscando corrigir falhas organizacionais ou institucionais que comprometem o funcionamento adequado do sistema[277]. A reestruturação proporcionada por essas decisões

[274]MARQUES; MENDES; BERGSTEIN, 2023, p. 7.
[275]*Ibidem*, p. 7.
[276]MARQUES; MENDES; BERGSTEIN, 2023, p. 7.
[277]BAMBIRRA, Tamara Brant; BRASIL, Deilton Ribeiro. Direito fundamental ao meio ambiente e o processo estrutural como meio adequado para sua tutela. **Revista de Direito Ambiental e Socioambientalismo**, v. 7, n. 1, p. 01-19, 2021. Disponível em:

tem como objetivo restabelecer a integridade social, garantindo seu pleno funcionamento e evitando novas violações.

A solução de um conflito é considerada estrutural quando demanda a modificação do funcionamento ou da própria estrutura social. A abordagem sistêmica é essencial, pois permite identificar as implicações e repercussões de cada decisão. Vitorelli[278] destaca que a eficácia das decisões estruturais depende da capacidade não apenas de enfrentar o problema imediato, mas também de promover mudanças profundas que impeçam sua repetição futura. Assim, é fundamental que as soluções adotadas não sejam apenas aparentes ou temporárias, mas duradouras e sustentáveis.

As decisões estruturais podem ser eficazes para lidar com a dinâmica dos padrões obscuros, de modo que, ao modificar a sistemática de violação de dados, como ocorre com o consentimento, que favorece a perpetuação desses padrões, as decisões estruturais produzem resultados concretos e permanentes, ao menos no sentido de tornar um dever a informação do usuário quanto às violações a que está sendo acometido. Como observa Vitorelli[279], é essencial que a intervenção considere tanto as causas quanto as consequências do problema, assegurando que a solução proposta seja efetiva e sustentável ao longo do tempo. Essa reorganização permite que as falhas estruturais não se repitam, garantindo a regularidade do funcionamento da estrutura, que no caso abordado é a sociedade em si.

O caráter performativo e qualitativo das decisões estruturais amplia o alcance das demandas judicializadas, proporcionando soluções que vão além dos limites tradicionais do processo judicial. Segundo Bambirra e Brasil[280], essas decisões trazem respostas inovadoras e eficazes, capazes de resolver situações complexas que não poderiam ser plenamente solucionadas por meios convencionais. Dessa forma, a intervenção estrutural soluciona o litígio imediato e também promove mudanças que afetam positivamente outros casos semelhantes.

---

https://www.indexlaw.org/index.php/Socioambientalismo/article/view/7567. Acesso em: 08 out. 2024. 2021, p. 2.

[278]VITORELLI, Edilson. Levando os conceitos a sério: processo estrutural, processo coletivo, processo estratégico e suas diferenças. **Revista de Processo**, v. 284, p. 333-369, 2018. Disponível em: https://www.academia.edu/download/60712061/vitorelli_-_LEVANDO_OS_CONCEITOS_A_SERIO_PROCESSO_ESTRUTURAL_PROCESSO_coletivo_processo_estrategico20190926-18785-1dqvis6.pdf. Acesso em: 08 out. 2024.

[279]*Ibidem*, p. 340.

[280]BAMBIRRA; BRASIL, 2021, p. 2.

O processo estrutural é um instrumento coletivo que visa a reorganização de estruturas burocráticas, públicas ou privadas, cujo funcionamento inadequado pode causar ou perpetuar violações de direitos. Ele envolve uma análise minuciosa do litígio, ouvindo todas as partes envolvidas, e a elaboração de um plano de intervenção que altere a forma de funcionamento da instituição. Esse plano pode ser implementado de forma compulsória ou negociada e deve ser acompanhado por uma avaliação contínua dos resultados, para garantir que os objetivos sociais sejam alcançados e que novas violações sejam evitadas. Se necessário, o plano pode ser ajustado e reimplementado, garantindo a eficácia do processo até que o problema seja resolvido[281].

As decisões estruturais são instrumentos essenciais para a efetivação dos direitos fundamentais assegurados pela Constituição Federal. Conforme apontado por Bambirra e Brasil[282], essas decisões exigem um debate aberto e participativo para que se alcance a melhor solução para cada caso. Ao promover a reorganização de padrões de funcionamento ineficazes e solucionar problemas estruturais, o processo estrutural garante que a proteção dos direitos fundamentais seja contínua e eficaz, evitando a perpetuação de falhas institucionais e assegurando o pleno funcionamento das organizações envolvidas.

As práticas estruturais, é importante esclarecer, são medidas voltadas para o futuro. Desse modo, não é devida uma análise unicamente do pleito apresentado. Essa ação só pode ser aplicada para situações de alta complexidade e deve ser implementada para uma reforma global que viabilize a redução de novas demandas. A prolação de decisões judiciais bem redigidas e que não apresentem um caráter genérico pode servir para prevenir e reparar os danos relacionados aos *dark patterns*.

Não se afasta, ainda, a necessidade de conscientização dos indivíduos sobre a existência de práticas de padrões obscuros aplicadas pelas plataformas digitais. Somente conhecendo os seus direitos, as práticas estruturais podem ser efetivamente aplicáveis pela população. Mostra-se devido, ainda, que sejam conduzidas investigações pelas autoridades competentes, com o intuito de mapear as principais práticas de *dark patterns* introduzidas pelas plataformas digitais.

Essas apurações são importantes para identificar os impactos dos padrões obscuros, bem como para estabelecer uma regulamentação efetiva para tais práticas, ainda que seja por

[281]VITORELLI, 2018, p. 340.
[282]BAMBIRRA; BRASIL, *op. cit.*, p. 10.

meio de medidas estruturais[283]. Há, ainda, a possibilidade de envolvimento direto dos operadores de internet no processo regulatório, o que pode também contribuir para a exequibilidade das soluções a serem definidas.

De qualquer modo, ainda que não sejam introduzidas medidas estruturais e/ou normas próprias, as autoridades consumeristas ou de proteção de dados podem editar guias e diretrizes para a abordagem dos padrões obscuros[284]. Essas práticas podem ser adotadas para garantia de um cenário de cooperação, de modo que os operadores de internet entendam a vedação aos *dark patterns* no Brasil.

Por fim, não se pode excluir a imprescindibilidade de adoção de um sistema de *"digital fairness by design".* Como estabelecido, o entendimento estrangeiro sobre *fairness* guarda uma relação direta com o princípio da boa-fé objetiva previsto no Código Civil, no Código de Defesa do Consumidor e na Lei Geral de Proteção de Dados Pessoais. Nesse formato, essa teoria desenvolvida pelo BEUC pode e deve ser aplicada no Brasil.

A ideia de *"digital fairness by design"* significa um importante precedente para a redução da aplicação de práticas que violam a boa-fé objetiva por plataformas digitais, tais como os padrões obscuros. Nesse formato de regulação, há uma modificação da forma de regulamentação posterior de determinada conduta por meio da aplicação de sanção. A teoria prevê que deve ser encorajada a adoção de uma postura proativa pelas plataformas digitais, com a antecipação e endereçamento, em momento anterior à ocorrência, de táticas manipuladoras[285].

O conceito de *"digital fairness by design"* advém da teoria formulada por Ann Cavoukian denominada como *"privacy by design"*. De acordo com a referida autora, devem ser introduzidos sete diferentes princípios em novos projetos de tecnologia com o intuito de adequação das plataformas à necessidade de proteção da privacidade dos envolvidos. Os listados preceitos são os seguintes: i) postura proativa e não reativa; enfoque na prevenção e não na contenção de danos; ii) privacidade como a modalidade básica aplicável; iii) privacidade instalada automaticamente na interface digital; iv) o objetivo é conseguir uma soma positiva no uso de meios que garantam a privacidade; v) proteção da privacidade durante

[283]BEUC, 2022, p. 12.
[284]*Ibidem*, p. 14.
[285]BEUC, 2024, p. 231.

todo o ciclo de uso de dados pessoais; vi) transparência e visibilidade e vii) respeito à privacidade dos usuários[286].

Essa teoria aborda, ainda, que a posição protetora dos agentes envolvidos deve estar alinhada com os objetivos das empresas que realizam o tratamento de dados pessoais, de modo que haja uma constante evolução entre a temática. A concepção de *"privacy by design"* encontra previsão expressa no artigo 25 da GDPR e se mostrou como uma eficiente ferramenta para garantir que a privacidade seja respeitada na concepção de novas tecnologias, processos e ferramentas digitais[287].

A efetividade, de acordo com a teoria de *"privacy by design"*, mostra-se como um ponto central. As ações introduzidas para salvaguarda do direito da privacidade dos usuários devem ser capazes de efetivamente alcançar as finalidades almejadas. As medidas que serão introduzidas pelos agentes merecem ser analisadas caso a caso. As plataformas digitais devem ser responsabilizadas pelos efeitos de suas ações e necessitam se adequar ao cumprimento das finalidades da lei em todos os aspectos das práticas que possam culminar em danos à privacidade dos usuários.

Essa concepção de *"by design"* merece atenção também na aplicação da boa-fé objetiva (*fairness*) pelas plataformas de internet[288]. Não é suficiente que as empresas adotem alguma medida para redução dos danos ocasionados pela adoção de padrões obscuros apenas após a regulamentação e a adoção de alguma penalidade pelos órgãos competentes. Na verdade, durante todo o procedimento de criação de interfaces tecnológicas, as empresas e cidadãos que atuam no setor devem levar em consideração a boa-fé objetiva e a impossibilidade de aplicação de práticas que manipulem a vontade real dos consumidores, tornando a tecnologia, desde a sua concepção, livre de artifícios manipuladores.

A imposição de multas e a adoção de um sistema regulatório de reparação de danos não é suficiente para garantir a proteção dos consumidores em face dos padrões obscuros. Isso ocorre por muitos fatores, sendo importante listar que, muitas vezes, as penas aplicadas não coíbem que os atores descumpram as determinações legislativas. Isto é, os ganhos que determinado agente pode ter pela aplicação de *dark patterns* pode ser significantemente maior

[286] *Ibidem*, p. 231.
[287] *Ibidem*, p. 232.
[288] *Ibidem*, p. 233.

que a penalidade imposta, sendo compensativo sujeitar-se ao risco de sanção, do ponto de vista econômico.

Nesse formato, a regulamentação no Brasil dos padrões obscuros deve observar a teoria de *"digital fairness by design".* Assim, todos os projetos que envolvam a venda de produtos e/ou prestação de serviços por plataformas digitais devem, desde a sua concepção, pautar-se pela necessidade de adoção de práticas que coíbam a manipulação das informações e da vontade dos clientes.

Ademais, as companhias merecem atuar de forma transparente e focada na proteção dos consumidores, especialmente aqueles mais vulneráveis, frente a práticas de padrões obscuros. Inclusive, deve-se levar em conta a dinamicidade da fragilidade dos agentes, dado que dependendo do ambiente há uma variação sobre quais atores podem ser entendidos como vulneráveis ou não.

Em conclusão, somente com a adoção de novas práticas e panoramas será possível proteger, de modo efetivo, os cidadãos brasileiros de táticas de padrões obscuros. É substancial, então, que seja dado o devido enfoque à matéria, com a adoção de teorias regulatórias, como a de *"digital fairness by design*", que sejam capazes de, por meio de uma cooperação entre atores públicos e privados, criar um ambiente justo e adequado para os consumidores do país.

CONCLUSÃO

A presente pesquisa concentrou-se na análise da validade do consentimento para o tratamento de dados pessoais no contexto das relações de consumo, com ênfase nas práticas conhecidas como *dark patterns*. O problema central abordado foi a influência negativa dessas práticas de design manipulativo sobre a autonomia dos titulares de dados, especialmente em situações nas quais o consentimento é obtido de forma ambígua ou por meio de artifícios que dificultam a compreensão do usuário. Nesse cenário, buscou-se investigar em que medida o uso dos *dark patterns* compromete a autodeterminação informativa, violando o consentimento válido e ferindo os direitos fundamentais à privacidade e à proteção de dados, conforme estabelecido na LGPD brasileira.

Com o objetivo de propor soluções regulatórias e aprimorar a proteção jurídica no Brasil, a pesquisa teve como foco a análise das Diretrizes nº 03/2022 da EDPB, que foram formuladas para orientar quanto ao uso dos *dark patterns* na União Europeia. O trabalho buscou verificar se a legislação e as práticas existentes garantem proteção efetiva aos consumidores ou se há lacunas que permitem a exploração de vulnerabilidades informacionais por meio de padrões obscuros. Ao longo da investigação, o objetivo principal foi identificar como superar essas falhas, promovendo maior transparência e conformidade no uso de dados pessoais, de forma a assegurar um equilíbrio nas relações entre consumidores e fornecedores no ambiente digital.

O desenvolvimento do regime jurídico de proteção de dados pessoais no Brasil reflete um processo contínuo de evolução influenciado por experiências internacionais e pela necessidade de regulamentar o uso crescente de dados no ambiente digital. Embora as origens das discussões sobre o tema sejam oriundas dos Estados Unidos, foi na Europa que a proteção de dados ganhou contornos mais robustos, com destaque para a Alemanha, pioneira na criação de normas específicas no período pós-guerra. O cenário europeu serviu como base para o GDPR, cuja aplicabilidade extraterritorial influenciou diretamente a LGPD no Brasil, promovendo a proteção da privacidade e a autodeterminação informativa.

O reconhecimento da proteção de dados pessoais como direito fundamental no Brasil foi consolidado por decisões do Supremo Tribunal Federal, tendo em seguida sido inserida na Constituição Federal pela Emenda Constitucional nº 115/2022. Antes da promulgação da LGPD, diplomas importantes como o Código de Defesa do Consumidor e o Marco Civil da Internet já previam salvaguardas relevantes, promovendo transparência e estabelecendo

normas de consentimento. A LGPD, por sua vez, ampliou essas proteções, abrangendo tanto o ambiente físico quanto o digital, e criou a Autoridade Nacional de Proteção de Dados para assegurar a aplicação da lei e supervisionar a conformidade dos agentes de tratamento de dados.

Além de fortalecer a posição do Brasil no cenário internacional, a harmonização da LGPD com o GDPR é essencial para garantir a segurança nas transferências de dados e facilitar o comércio global. A ANPD desempenha um papel estratégico ao avaliar a adequação de normas estrangeiras e assegurar que o tratamento de dados respeite padrões de proteção robustos. Ao se alinhar com esses princípios internacionais, o Brasil não apenas protege os direitos dos cidadãos, mas também posiciona suas empresas para competir de forma ética e eficiente no mercado digital global, respondendo aos desafios contemporâneos apresentados pela inteligência artificial e pelo uso intensivo de Big Data.

A autodeterminação informativa é um dos pilares centrais da proteção de dados pessoais, representando o controle do indivíduo sobre suas informações e a capacidade de decidir sobre seu uso e disseminação. Originado na jurisprudência alemã, o conceito foi formulado como uma resposta à necessidade de proteção frente ao processamento automatizado de dados e sua capacidade de traçar perfis detalhados de indivíduos. No Brasil, esse direito encontra amparo na LGPD e é associado à dignidade da pessoa humana e ao livre desenvolvimento da personalidade, refletindo o equilíbrio necessário entre a autonomia privada e a proteção contra abusos nas relações sociais e comerciais.

Embora o consentimento seja um instrumento essencial para a concretização da autodeterminação informativa, ele não pode ser visto como absoluto. A regulação precisa considerar que, em certos contextos, a autonomia do titular de dados é limitada por pressões econômicas, sociais ou tecnológicas, comprometendo a liberdade de escolha. Assim, a proteção de dados vai além da simples manifestação de vontade e envolve o desenvolvimento de mecanismos legais e regulatórios que assegurem a privacidade contextual e a integridade do tratamento de dados. Dessa forma, a proteção de dados pessoais é compreendida como um direito da personalidade e um direito fundamental, transcendendo o consentimento individual para promover um equilíbrio entre interesses privados e o bem comum na sociedade digital contemporânea.

A exploração de dados pessoais na era digital evidencia uma relação de dependência entre indivíduos e plataformas online, contexto em que o consentimento para coleta e

processamento de dados se torna essencial para acesso a serviços. No entanto, essa prática frequentemente apresenta limitações na liberdade de escolha dos usuários, uma vez que, na ausência de alternativas viáveis, o consentimento torna-se uma mera formalidade. A vulnerabilidade informacional intensifica esse desequilíbrio, fazendo com que o consumidor aceite termos de uso que nem sempre compreende completamente, gerando preocupações sobre a validade e autenticidade desse consentimento. Nesse contexto, o direito à revogação do consentimento, garantido pela LGPD, emerge como uma ferramenta crucial para mitigar esses problemas, conferindo maior controle ao titular sobre seus dados ao permitir a interrupção do tratamento sem necessidade de se justificar, impedindo uma burocratização do processo.

Além disso, a coleta massiva e a utilização de dados comportamentais e emocionais por meio de algoritmos e inteligência artificial refletem a "sociedade do controle", em que empresas moldam comportamentos e decisões de consumo com base em perfis detalhados dos usuários. Essa prática, aliada a estratégias como design viciante e publicidade direcionada, transforma dados em valiosos recursos econômicos e levanta questões sobre a violação da liberdade de escolha. A LGPD e o CDC reconhecem a necessidade de proteger os usuários contra abusos decorrentes dessas práticas, destacando a importância da transparência e da explicação sobre o uso de dados. Nesse cenário, é essencial promover um equilíbrio entre inovação e privacidade, assegurando que a tomada de decisões automatizadas respeite a integridade e a autonomia do consumidor, evitando a exclusão social e econômica dos indivíduos mais vulneráveis.

O comércio eletrônico intensificou a vulnerabilidade do consumidor no ambiente digital, transformando padrões de consumo e criando relações econômicas e sociais. A globalização e a digitalização não apenas facilitaram a compra de bens e serviços, mas também introduziram desafios inéditos. Entre eles, destaca-se a superexposição de dados pessoais e o uso extensivo de tecnologias como algoritmos e inteligência artificial, que afetam a autonomia dos consumidores e moldam suas decisões de forma estratégica. Nesse cenário, a vulnerabilidade informacional torna-se especialmente relevante, exigindo a criação de mecanismos legais e regulatórios que assegurem maior transparência e proteção aos dados coletados.

A transformação digital também impactou a forma como as empresas utilizam dados pessoais para personalizar ofertas e serviços, criando uma economia orientada pela informação. A individualização do consumidor, baseada na análise de preferências e

comportamentos, apresenta vantagens, mas também riscos de manipulação e discriminação. Assim, surge a necessidade de um equilíbrio entre a personalização das ofertas e a proteção da privacidade, garantindo que o uso de dados seja transparente e esteja alinhado com as expectativas legítimas dos consumidores, conforme exigido pela LGPD.

A obtenção de consentimento válido é fundamental para a conformidade com a LGPD, representando uma forma de assegurar a autodeterminação informativa dos consumidores. No entanto, o consentimento precisa ser livre e inequívoco, com informações claras sobre a finalidade do tratamento de dados. A legislação brasileira também prevê a possibilidade de revogação desse consentimento, assegurando que o consumidor mantenha controle contínuo sobre seus dados, conforme explicado. A boa-fé objetiva, princípio compartilhado pelo CDC e pela LGPD, impõe aos controladores de dados o dever de agir de forma transparente e leal, respeitando as expectativas dos titulares.

A proteção de dados é vista como um direito fundamental do consumidor, conectando-se ao dever do Estado de defender o indivíduo contra abusos e discriminações no mercado. A gestão segura e responsável das informações pessoais inclui não apenas a prevenção de violações de segurança, mas também a limitação do tempo de armazenamento dos dados e a necessária gerência e responsabilidade sobre eles. Isso garante que os dados não sejam retidos além do necessário, evitando riscos futuros para o titular. Ademais, a transparência deve ser um princípio central na comunicação entre empresas e consumidores, fortalecendo a confiança nas relações digitais.

Denota-se ainda que a cooperação entre o setor público e privado é essencial para enfrentar os desafios da proteção de dados no comércio eletrônico. A autorregulação regulada se apresenta como uma solução viável para promover boas práticas no mercado, aliando inovação e responsabilidade. A ANPD desempenha um papel crucial nesse processo, orientando e supervisionando as empresas na adoção de padrões éticos e legais. Assim, a proteção dos dados pessoais e o respeito à privacidade não apenas garantem a confiança dos consumidores, mas consolidam a segurança jurídica e a eficiência nas relações de consumo digitais.

De modo a oferecer soluções concretas, analisou-se o Guia nº 3/2022, elaborado pelo European Data Protection Board (EDPB), que fornece diretrizes sobre o reconhecimento e a prevenção de padrões obscuros, práticas manipuladoras que influenciam negativamente as decisões dos usuários em relação ao processamento de seus dados pessoais. Tais padrões,

também conhecidos como "*dark patterns*", são definidos como estratégias de design de interfaces que induzem usuários a tomar decisões involuntárias ou prejudiciais, desrespeitando as normas estabelecidas pelo GDPR[289].

O guia classifica esses padrões em seis categorias: "sobrecarga" (*overloading*), "ignorar" (*skipping*), "agitação" (*stirring*), "dificultar" (*hindering*), "inconstante" (*fickle*) e "deixar no escuro" (*left in the dark*), que refletem diferentes formas de manipulação, como a apresentação excessiva de informações, a ocultação de dados relevantes ou a dificuldade de encontrar opções relacionadas à privacidade[290]. O objetivo é assegurar que as plataformas digitais sigam princípios como autonomia, transparência, verdade e o balanceamento de poder na relação com os titulares dos dados[291].

O EDPB também propõe boas práticas que visam promover a transparência e a compreensão das políticas de privacidade, como a disponibilização de atalhos para informações sobre o processamento de dados, a apresentação de todas as opções de privacidade em uma única aba e a clareza na comunicação com os usuários[292]. Além disso, destaca-se a necessidade de atenção especial aos grupos vulneráveis, como crianças, idosos e pessoas com deficiência, que podem ter maior dificuldade de identificar padrões obscuros e, portanto, requerem proteção adicional.

Apesar de o Guia nº 3/2022 ter trazido avanços na regulamentação dos padrões obscuros, ainda existem desafios significativos na implementação efetiva dessas práticas. A complexidade técnica dos padrões obscuros e a falta de uma abordagem padronizada dificultam sua identificação e fiscalização. Portanto, o sucesso dessas diretrizes dependerá de uma cooperação contínua entre reguladores, plataformas digitais e consumidores, bem como de ações que garantam o pleno respeito aos direitos dos titulares de dados.

Com o estudo, foi possível observar que o princípio da boa-fé objetiva exerce um papel fundamental no Direito do Consumidor e no Direito Privado em geral, como previsto no artigo 4º, III, do Código de Defesa do Consumidor (CDC), orientando a análise das relações entre fornecedores e consumidores. Esse princípio exige condutas leais, transparentes e respeitosas, o que vai além de uma análise subjetiva das intenções individuais, pois impõe um padrão ético

[289]EDPB, 2023, p. 2.
[290]*Ibidem*, p. 2.
[291]*Ibidem*, p. 13-14.
[292]*Ibidem*, p. 73.

e de correção na execução de contratos e na interação entre as partes[293]. Além disso, sua introdução pelo CDC em 1990 e sua posterior incorporação pelo Código Civil de 2002 estabeleceram uma tríplice função: interpretar contratos de forma justa, integrar deveres acessórios além das obrigações principais e restringir abusos contratuais (Tepedino; Schreiber, 2003, p. 144).

Notou-se que, no âmbito da proteção de dados pessoais, a boa-fé objetiva também se destaca, sendo princípio fundamental da Lei Geral de Proteção de Dados (LGPD), que estabelece condutas transparentes e corretas no tratamento de dados. O princípio da boa-fé objetiva, aplicado à proteção de dados, busca assegurar que informações claras e precisas sejam fornecidas aos titulares, para que possam tomar decisões informadas e conscientes[294]. Nesse contexto, Bruno Bioni destaca que a confiança dos titulares está intrinsecamente ligada à observância desse princípio, que se aplica tanto ao tratamento de informações públicas quanto privadas, sendo essencial para equilibrar as exigências de proteção à privacidade e segurança dos dados[295].

A boa-fé objetiva encontra similaridade com o conceito de "*digital fairness*" proposto pelo *Bureau Européen des Unions de Consommateurs* (BEUC), que visa proteger consumidores no ambiente digital contra práticas que exploram vulnerabilidades e manipulam escolhas. A ideia de "*digital fairness by design*" propõe que, desde a concepção dos produtos e serviços digitais, sejam adotadas práticas transparentes e leais, de modo a evitar ações abusivas ou manipulativas[296]. Essa abordagem alinha-se à necessidade de aplicar a boa-fé objetiva nos ambientes digitais, prevenindo práticas que possam prejudicar os consumidores e usuários.

Os padrões obscuros, ou *dark patterns*, representam um sério risco para os usuários de plataformas digitais, uma vez que impactam diretamente sua capacidade de tomar decisões conscientes. Tais práticas comprometem a autonomia, a confiança e a segurança dos consumidores dentro desses ecossistemas digitais, o que aponta para uma necessidade urgente de regulamentação. Padrões obscuros são ações de design persuasivo que manipulam a experiência do usuário para direcioná-lo a decisões que não necessariamente tomaria de forma consciente, como a adição automática de produtos ao carrinho de compras, confirmação

[293]MIRAGEM, 2024, p. 114.
[294]FRAZÃO; TEPEDINO; OLIVA, 2020, (n.p.).
[295]BIONI, 2021, p. 234.
[296]BEUC, 2024, p. 166.

automática de assinaturas em custos ocultos ou utilização de ferramentas que criam falsas indicações de escassez. Essas táticas são altamente prejudiciais ao consumidor e demandam mecanismos regulatórios claros e efetivos.

Nessa dinâmica, buscando oferecer uma resposta ao problema de pesquisa proposto, qual seja "como o uso de *dark patterns* pode comprometer a validade do consentimento obtido do titular no âmbito das relações de consumo, e consequentemente afetar o seu direito à proteção de dados pessoais e o que pode ser feito para contornar essa situação", tem-se a seguinte proposta.

Pode-se dizer que foi demonstrado que os *dark patterns* comprometem a validade do consentimento do titular de dados na medida em que lhes retira a autonomia, através de processos de manipulação, impedindo que o consentimento seja livre, informado e inequívoco, como determina o inciso XII do art. 5º da LGPD. Nessa esteira, a partir de práticas de condução e manipulação, bem como pelo uso de vieses que modulam o comportamento do usuário, não há que se falar em manifestação livre, tampouco informada.

Em seguida, quanto ao questionamento do que pode ser feito para contornar essa situação, foram apresentadas duas propostas. A primeira, focada na utilização de ações coletivas, com um viés estrutural, isto é, a busca pela construção de uma solução na via jurisdicional, que leve em consideração o diálogo das fontes, entre o CDC, o Código Civil e a LGPD, de modo a impedir que o consentimento oferecido pelo titular para o tratamento de dados pessoais, quando diante da utilização de *dark patterns*, seja considerado válido, impedindo o processo, bem como penalizando a empresa responsável pelo feito.

Em seguida, uma segunda proposta, baseada na observância de que no cenário brasileiro, ainda que existam princípios amplos como a boa-fé objetiva e legislações que tratam do direito civil, do consumidor e da proteção de dados, falta uma norma específica que regule os padrões obscuros. Atualmente, a vedação de práticas que prejudiquem a lealdade das relações se encontra pulverizada em diferentes normativos, dificultando a proteção do usuário. Ao se comparar com a União Europeia, onde a regulação sobre o tema se dá por meio de normas de alcance específico, observa-se que o Brasil carece de uma abordagem mais consolidada para lidar com essas práticas, tendo em vista que essa lacuna normativa pode permitir que certas condutas não se encaixem em quaisquer padrões legislativos existentes.

Considerando a ausência de uma legislação específica no Brasil, é fundamental a edição de normas claras e aplicáveis ao contexto nacional. A experiência de outros países,

como as recomendações do *Bureau Européen des Unions de Consommateurs* (BEUC), pode servir de modelo para a elaboração de uma regulação eficiente. Além disso, as autoras Claudia Lima Marques, Laura Schertel Mendes e Laís Bergstein sugerem a implementação de medidas estruturais no combate aos padrões obscuros, por meio do uso de ações coletivas de processo civil, que, embora possuam limitações quanto à proteção dos direitos dos cidadãos, podem ser mais efetivas quando pautadas por decisões estruturais, como é feito na doutrina norte-americana.

As ações estruturais, ao contrário do que alegam alguns críticos, não violam o princípio da separação dos poderes, pois o Judiciário deve assegurar que a aplicação de uma decisão tenha reflexos práticos em todo o território. Esse tipo de abordagem tem potencial para prevenir a ocorrência de práticas de padrões obscuros, garantindo que as empresas sejam responsabilizadas não apenas em casos individuais, mas de forma sistêmica e abrangente. A adoção dessas medidas encontra amparo na legislação consumerista brasileira, que, em seus artigos 83 e 84, prevê a utilização de todos os mecanismos necessários para resguardar os interesses dos consumidores.

Para que as ações estruturais sejam verdadeiramente eficazes, é fundamental que os consumidores sejam informados sobre a existência de padrões obscuros. A conscientização é um pilar essencial para que a população exija a aplicação efetiva dessas medidas. Além disso, investigações e mapeamentos realizados pelas autoridades competentes podem identificar práticas prejudiciais adotadas por plataformas digitais, estabelecendo uma base sólida para a elaboração de regulamentações. A cooperação entre reguladores, plataformas digitais e usuários pode contribuir para a criação de guias práticos que delineiam as condutas a serem evitadas no ambiente online.

Finalmente, entende-se que é crucial adotar uma abordagem de "*digital fairness by design*", alinhando a proteção dos consumidores com práticas justas e transparentes por parte das empresas. Inspirada na teoria de "*privacy by design*", essa abordagem promove a prevenção de danos por meio do design inicial das interfaces digitais, buscando antecipar e endereçar práticas manipuladoras antes que ocorram. A adoção dessa postura proativa por parte das plataformas digitais tem o potencial de criar um ambiente mais seguro e justo para os consumidores brasileiros, garantindo a proteção efetiva de seus direitos e interesses. Em conclusão, para proteger efetivamente os cidadãos brasileiros dos riscos associados aos padrões obscuros, é imprescindível uma abordagem regulamentar abrangente e colaborativa, centrada na equidade digital e no respeito à autonomia do consumidor.

REFERÊNCIAS

ADORNO, Theodor. **Dialética do esclarecimento**. Editora Schwarcz-Companhia das Letras, 1985.

AMARAL, Francisco. **Direito Civil**: introdução. 6.ed. rev. atual. e aum. Rio de Janeiro: Renovar, 2006.

BAMBIRRA, Tamara Brant; BRASIL, Deilton Ribeiro. Direito fundamental ao meio ambiente e o processo estrutural como meio adequado para sua tutela. **Revista de Direito Ambiental e Socioambientalismo**, v. 7, n. 1, p. 01-19, 2021. Disponível em: https://www.indexlaw.org/index.php/Socioambientalismo/article/view/7567. Acesso em: 08 out. 2024.

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

BEUC (The European Consumer Organisation). ***"Dark Patterns" and the EU Consumer Law Acquis***. Recommendations for better enforcement and reform. Ref: BEUC-X-2022-013 - 07/02/2022. Disponível em: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf. Acesso em: 01 set. 2024.

BEUC (The European Consumer Organisation). ***"Digital Fairness for Consumers"***. Natali Helberger, Betül Kas, Hans-W. Micklitz, Monika Namysłowska, Laurens Naudts, Peter Rott, Marijn Sax, Michael Veale. Brussels, March 2024. Disponível em: https://discovery.ucl.ac.uk/id/eprint/10189356/. Acesso em: 05 set. 2024.

BIONI, Bruno. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento.** In: Minha Biblioteca, (3rd edição). Grupo GEN, 2021.

BRASIL. **Constituição Federal de 5 de outubro de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm. Acesso em: 20 mai. 2023.

_____. **Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 20 mai. 2023.

_____. **Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 20 mai. 2023. Acesso em: 01 set. 2024.

_____. **Lei nº 12.965, de 23 de abril de 2014. Lei do Marco Civil da Internet**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 mai. 2023.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mai. 2023.

BRIGNULL, Harry. **Types of deceptive pattern.** Disponível em: https://www.deceptive.design/types. Acesso em: 31 ago. 2024.

CABRAL, Érico de Pina. A "autonomia" no direito privado. In: **Revista de Direito Privado. São Paulo: Revista dos Tribunais**, 19(5)83-129, jul/set 2004.

CARVALHO, Diógenes Faria de. **A boa-fé objetiva nos contratos de consumo**. Dissertação apresentada como requisito para a conclusão do Mestrado em Direito das Relações Econômico-Empresariais. Universidade de Franca - UNIFRAN: São Paulo, 2006.

DE MARCO, Cristhian Magnus. **Elementos sobre a autonomia privada e sua relação com o mínimo existencial na teoria dos direitos fundamentais**. *In*: BAEZ, Narciso Leandro Xavier Baez; CASSEL, Douglas (Orgs.). A realização e a proteção internacional dos Direitos Humanos: desafios do século XXI. Joaçaba: Ed. UNOESC, p. 246-59, 2011.

DE SOUSA, Rosilene Paiva Marinho; DA SILVA, Paulo Henrique Tavares. Proteção de dados pessoais e os contornos da autodeterminação informativa. **Informação & Sociedade**, v. 30, n. 2, 2020.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. *In*: Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2020.

EUROPEAN PARLIAMENT. **Resolução do Parlamento Europeu de 12 de dezembro de 2023 sobre o design viciante de serviços em linha e a proteção do consumidor no mercado único da UE (2023/2043(INI)).** 2023. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.html. Acesso em: 15 set. 2024.

FERNANDES, Sofia. O que é design viciante e por que a UE quer limitar seu uso? **Deutsche Welle**. Direitos Humanos - Alemanha. Publicado em 12/06/2024. Disponível em: https://p.dw.com/p/4gwbI. Acesso em: 15 set. 2024.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2020.

FREDERICO, Elias. **O que é Marketing.** Antenna Web, v. 4, n. 1, 2008.

GADELHA, Gisela Pimenta. **Boas práticas e governança corporativa**. in: Manual do DPO. São Paulo: Thomson Reuters Brasil, 2021.

GRAEF, Inge. **The EU regulatory patchwork for dark patterns: an illustration of an inframarginal revolution in European law?.** In: Toward an Inframarginal Revolution: Markets as Wealth Distributors. Cambridge University Press. 2023.

LIMA, Patrícia Raposo Santana; DE CASTRO SALGADO, Luciana Cardoso. Estratégias de comunicação do Consentimento Informado e rastros de Padrões Obscuros no Instagram. In: **Anais do III Workshop sobre as Implicações da Computação na Sociedade**. SBC, 2022. p. 40-54.

LIRA, Mydyã. **Termos de uso: conheça seus requisitos e sua finalidade**. EJUDI, Ceará: 2023. Disponível em: https://ejudi.com.br/termo-de-uso-finalidade/. Acesso em: 20 set. 2024.

LOCATELLI, Liliana; DE PAIVA SIMON, Cláudio Antonio. A vulnerabilidade do consumidor ante os ambientes virtuais: o caso dos sítios de aproximação. **Revista Direitos Culturais**, v. 3, n. 4, p. 157-168, 2008.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Européia (LGPD e GDPR) e seus respectivos instrumentos de *Enforcement.* In: **Revista do programa de Direito da União Européia**. FGV: Rio de Janeiro, 2021.

LÉVY, Pierre. **A conexão planetária**. O mercado, o ciberespaço, a consciência. 1ª reimpressão. Tradução de Maria Lucia Homem e Ronaldo Entler. São Paulo: Ed. 34, 2003.

LEISER, Mark. **Illuminating Manipulative Design: From "Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive.** Loyola Consumer Law Review, v. 34, p. 484-528, 2022.

LUKOFF, Kai; HINIKER, Alexis; GRAY, Colin M.; MATHUR, Arunesh; CHIVUKULA, Shruthi. **What can CHI Do About Dark Patteens?.** In: CHI ’21 Extended Abstracts. Japão, 2021.

MAGALHÃES NETO, F. B. de .; MAGALHÃES, L. B. B. de . A evolução do direito do consumidor e o comércio eletrônico: abordagem pelo direito internacional. **Revista de Direito da ADVOCEF**, [S. l.], v. 13, n. 25, p. 123–142, 2017. Disponível em: https://revista.advocef.org.br/index.php/ra/article/view/318. Acesso em: 05 mai. 2024.

MALDONADO, Viviane Nóbrega. **Contextualização da proteção de dados no Brasil e no mundo e elementos essenciais da LGPD**. *In*: Manual do DPO. São Paulo: Thomson Reuters Brasil, 2021.

MARQUES, Cláudia Lima; MUCELIN, Guilherme Antônio B. **Inteligência artificial e “opacidade” no consumo:** a necessária revalorização da transparência para a proteção do consumidor. In: O direito civil na era da inteligência artificial. São Paulo: Thomson Reuters Brasil, 2020.

MARQUES, Cláudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. Dark patterns e padrões comerciais escusos. **Revista de Direito do Consumidor**. vol. 145. ano 32. p. 295-316. São Paulo: Ed. RT, jan./fev. 2023. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/174455. Acesso em: 05 mai. 2024.

MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental**. Ed. Saraiva: São Paulo, 2014.

MENDES, Laura Schertel Ferreira. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. **Revista de Direito do Consumidor.** Revista dos Tribunais: São Paulo, 2015.

MENDES, Laura Schertel Ferreira. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. São Paulo: **Revista dos Tribunais**, 2016.

MENDES, Laura Schertel Ferreira. BIONI, Bruno Ricardo. O Regulamento europeu de proteção de dados pessoais e a Lei Geral de Proteção de Dados brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**: São Paulo, 2019.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 12, n. 39, p. 185-216, 2018.

MENDES, Laura Schertel. FONSECA, Gabriel C. Soares da. STF reconhece direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor** | vol. 130/2020 | p. 471 - 478 | Jul - Ago / 2020. Disponível em: https://www.researchgate.net/publication/344381892_STF_reconhece_direito_fundamental_a_protecao_de_dados. Acesso em: 23 jul. 2023.

MICHAELS, Jordyn. **Pathways to the Light: Realistic Tactics to Address Dark Patterns.** Rutgers Computer and Technology Law Journal 49, n. 1: Chicago, p. 176 a 206, 2022.

MIRAGEM, Bruno. **Curso de Direito do Consumidor.** 6. ed. São Paulo: Revista dos Tribunais, 2016.

MIRAGEM, Bruno Nubens Barbosa. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor**. São Paulo: Revista dos Tribunais, 2019.

MIRAGEM, Bruno. **Curso de Direito do Consumidor**. 9. ed. Rio de Janeiro: Editora Forense, 2024.

MONTANARO, Domingo. **Medidas técnicas e administrativas para a segurança da informação**. In: Manual do DPO – Data Protection Officer. São Paulo: Revista dos Tribunais: 2021.

NUNES, Luiz Antônio Rizzato. **Comentários ao código de defesa do consumidor.** In: Minha Biblioteca, (8th edição). Grupo GEN, 2015.

PAIVA, Ana Lorena Nascimento; BISPO, Ronaldo. **Emojis, as emoções representadas graficamente no ciberespaço**. *In:* Intercom-XIX Congresso de Ciências da Comunicação na Região Nordeste. 2017.

PENTEADO, Luciano de Camargo. Figuras parcelares da boa-fé objetiva *e venire contra factum proprium*. **Revista de direito privado**, v. 27, n. 1, p. 252-278, 2006

PINTO, Carlos Alberto Mota. **Teoria Geral do Direito Civil**. 4.ed. por António Pinto Monteiro e Paulo Mota Pinto. Coimbra: Coimbra Editora, 2005.

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

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

SARLET, Ingo Wolfgang. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental**. Conjur, 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental. Acesso em: 29 jul. 2023.

SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. 2. ed. Rio de Janeiro: Lumen Juris, 2009.

SILVA, Alexandre Assunção. A proteção pelo MPF dos dados pessoais dos usuários da internet. *In*: BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 3. **Sistema brasileiro de proteção e acesso a dados pessoais: Análise de dispositivos da Lei de acesso à informação, da Lei de identificação civil, da Lei do marco civil da internet e da Lei nacional de proteção de dados** - Brasília: MPF, 85p. - (Roteiro de Atuação; v. 3), 2019. Disponível em: http://hdl.handle.net/11549/189803. Acesso em: 28 abr. 2023.

SILVA, Lucas Gonçalves; MELO, Bricio Luis da Anunciação; KFOURI, Gustavo. A LEI GERAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO DE CONCRETIZAÇÃO DA AUTONOMIA PRIVADA EM UM MUNDO CADA VEZ MAIS TECNOLÓGICO. **Revista Jurídica**, [S.l.], v. 3, n. 56, p. 354 - 377, jul. 2019. ISSN 0103-3506. Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3581/371371972. Acesso em: 23 jul. 2023. doi:http://dx.doi.org/10.26668/revistajur.2316-753X.v3i56.3581.

SIQUEIRA, . N.; CONTIN,. C.; BARUFI,. B.; LEHFELD,. de S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD . **Revista Eletrônica Pesquiseduca**, [S. l.], v. 13, n. 29, p. 236–255, 2021. DOI: 10.58422/repesq.2021.e1029. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 20 mai. 2023.

SOUZA, Joyce; AVELINO, Rodolfo; DA SILVEIRA, Sérgio Amadeu. **A Sociedade de Controle: Manipulação e modulação nas redes sociais**. Hedra: São Paulo, 2018.

TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. **Manual de direito do consumidor**: direito material e processual. rev. e atual. Rio de Janeiro: Método, 2017.

TEPEDINO, Gustavo; SCHREIBER, Anderson. Os efeitos da Constituição em relação à Cláusula da Boa-fé no Código de Defesa do Consumidor e no Código Civil. R**evista da EMERJ**, v. 6, n. 23, Rio de Janeiro, 2003.

THE EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them"**. Version 2.0. Adopted on 14 February 2023. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.

VERBICARO, Dennis; VIEIRA, Janaína. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. **Revista de Direito do Consumidor**: São Paulo, 2021.

VERBICARO, Dennis; RODRIGUES, Lays; ATAÍDE, Camile; Desvendando a vulnerabilidade comportamental do consumidor: uma análise jurídico-psicológica do assédio de consumo. **Revista de Direito do Consumidor**, 119. 349-384, São Paulo, 2018.

VITORELLI, Edilson. Levando os conceitos a sério: processo estrutural, processo coletivo, processo estratégico e suas diferenças. **Revista de Processo**, v. 284, p. 333-369, 2018. Disponível em: https://www.academia.edu/download/60712061/vitorelli_-_LEVANDO_OS_CONCEITOS_A_SERIO_PROCESSO_ESTRUTURAL_PROCESSO_coletivo_processo_estrategico20190926-18785-1dqvis6.pdf. Acesso em: 08 out. 2024.

XIMENES, Mariana. **O que é streaming?** Hardware.com. 2021. Disponível em: https://www.hardware.com.br/artigos/o-que-e-streaming/. Acesso em: 20 set. 2024.
ADORNO, Theodor. **Dialética do esclarecimento**. Editora Schwarcz-Companhia das Letras, 1985.

AMARAL, Francisco. **Direito Civil**: introdução. 6.ed. rev. atual. e aum. Rio de Janeiro: Renovar, 2006.

BAMBIRRA, Tamara Brant; BRASIL, Deilton Ribeiro. Direito fundamental ao meio ambiente e o processo estrutural como meio adequado para sua tutela. **Revista de Direito Ambiental e Socioambientalismo**, v. 7, n. 1, p. 01-19, 2021. Disponível em: https://www.indexlaw.org/index.php/Socioambientalismo/article/view/7567. Acesso em: 08 out. 2024.

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

BEUC (The European Consumer Organisation). ***"Dark Patterns" and the EU Consumer Law Acquis***. Recommendations for better enforcement and reform. Ref: BEUC-X-2022-013 - 07/02/2022. Disponível em: https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-013_dark_patters_paper.pdf. Acesso em: 01 set. 2024.

BEUC (The European Consumer Organisation). ***"Digital Fairness for Consumers"***. Natali Helberger, Betül Kas, Hans-W. Micklitz, Monika Namysłowska, Laurens Naudts, Peter Rott, Marijn Sax, Michael Veale. Brussels, March 2024. Disponível em: https://discovery.ucl.ac.uk/id/eprint/10189356/. Acesso em: 05 set. 2024.

BIONI, Bruno. **Proteção de Dados Pessoais - A Função e os Limites do Consentimento.** In: Minha Biblioteca, (3rd edição). Grupo GEN, 2021.

BRASIL. **Constituição Federal de 5 de outubro de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituiçao.htm. Acesso em: 20 mai. 2023.

_____. **Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor**. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 20 mai. 2023.

_____. **Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil**. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 20 mai. 2023. Acesso em: 01 set. 2024.

_____. **Lei nº 12.965, de 23 de abril de 2014. Lei do Marco Civil da Internet**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 mai. 2023.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 mai. 2023.

BRIGNULL, Harry. **Types of deceptive pattern.** Disponível em: https://www.deceptive.design/types. Acesso em: 31 ago. 2024.

CABRAL, Érico de Pina. A "autonomia" no direito privado. In: **Revista de Direito Privado. São Paulo: Revista dos Tribunais**, 19(5)83-129, jul/set 2004.

CAMPOS, Ricardo. **Metamorfoses do direito global:** sobre a interação entre direito, tempo e tecnologia. São Paulo, SP: Editora Contracorrente, 2022.

CARVALHO, Diógenes Faria de. **A boa-fé objetiva nos contratos de consumo**. Dissertação apresentada como requisito para a conclusão do Mestrado em Direito das Relações Econômico-Empresariais. Universidade de Franca - UNIFRAN: São Paulo, 2006.

DE MARCO, Cristhian Magnus. **Elementos sobre a autonomia privada e sua relação com o mínimo existencial na teoria dos direitos fundamentais**. *In*: BAEZ, Narciso Leandro Xavier Baez; CASSEL, Douglas (Orgs.). A realização e a proteção internacional dos Direitos Humanos: desafios do século XXI. Joaçaba: Ed. UNOESC, p. 246-59, 2011.

DE SOUSA, Rosilene Paiva Marinho; DA SILVA, Paulo Henrique Tavares. Proteção de dados pessoais e os contornos da autodeterminação informativa. **Informação & Sociedade**, v. 30, n. 2, 2020.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. *In*: Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2020.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. *In*: Tratado de Proteção de Dados Pessoais. CORRÊA, Adriana Espíndola… [*et. al.*]; coordenação Danilo Doneda …[*et. al.*]. - 2 ed. - Rio de Janeiro: Forense, 2023.

EUROPEAN PARLIAMENT. **Resolução do Parlamento Europeu de 12 de dezembro de 2023 sobre o design viciante de serviços em linha e a proteção do consumidor no mercado único da UE (2023/2043(INI)).** 2023. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0459_EN.html. Acesso em: 15 set. 2024.

FERNANDES, Sofia. O que é design viciante e por que a UE quer limitar seu uso? **Deutsche Welle**. Direitos Humanos - Alemanha. Publicado em 12/06/2024. Disponível em: https://p.dw.com/p/4gwbI. Acesso em: 15 set. 2024.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2020.

FREDERICO, Elias. **O que é Marketing.** Antenna Web, v. 4, n. 1, 2008.

GADELHA, Gisela Pimenta. **Boas práticas e governança corporativa**. in: Manual do DPO. São Paulo: Thomson Reuters Brasil, 2021.

GRAEF, Inge. **The EU regulatory patchwork for dark patterns: an illustration of an inframarginal revolution in European law?.** In: Toward an Inframarginal Revolution: Markets as Wealth Distributors. Cambridge University Press. 2023.

LIMA, Patrícia Raposo Santana; DE CASTRO SALGADO, Luciana Cardoso. Estratégias de comunicação do Consentimento Informado e rastros de Padrões Obscuros no Instagram. In: **Anais do III Workshop sobre as Implicações da Computação na Sociedade**. SBC, 2022. p. 40-54.

LIRA, Mydyã. **Termos de uso: conheça seus requisitos e sua finalidade**. EJUDI, Ceará: 2023. Disponível em: https://ejudi.com.br/termo-de-uso-finalidade/. Acesso em: 20 set. 2024.

LOCATELLI, Liliana; DE PAIVA SIMON, Cláudio Antonio. A vulnerabilidade do consumidor ante os ambientes virtuais: o caso dos sítios de aproximação. **Revista Direitos Culturais**, v. 3, n. 4, p. 157-168, 2008.

LORENZON, Laila Neves. Análise comparada entre regulamentações de dados pessoais no Brasil e na União Européia (LGPD e GDPR) e seus respectivos instrumentos de *Enforcement.* In: **Revista do programa de Direito da União Européia**. FGV: Rio de Janeiro, 2021.

LÉVY, Pierre. **A conexão planetária**. O mercado, o ciberespaço, a consciência. 1ª reimpressão. Tradução de Maria Lucia Homem e Ronaldo Entler. São Paulo: Ed. 34, 2003.

LEISER, Mark. **Illuminating Manipulative Design: From "Dark Patterns" to Information Asymmetry and the Repression of Free Choice under the Unfair Commercial Practices Directive.** Loyola Consumer Law Review, v. 34, p. 484-528, 2022.

LUKOFF, Kai; HINIKER, Alexis; GRAY, Colin M.; MATHUR, Arunesh; CHIVUKULA, Shruthi. **What can CHI Do About Dark Patteens?.** In: CHI ’21 Extended Abstracts. Japão, 2021.

MAGALHÃES NETO, F. B. de .; MAGALHÃES, L. B. B. de . A evolução do direito do consumidor e o comércio eletrônico: abordagem pelo direito internacional. **Revista de Direito da ADVOCEF**, [S. l.], v. 13, n. 25, p. 123–142, 2017. Disponível em: https://revista.advocef.org.br/index.php/ra/article/view/318. Acesso em: 05 mai. 2024.

MALDONADO, Viviane Nóbrega. **Contextualização da proteção de dados no Brasil e no mundo e elementos essenciais da LGPD**. *In*: Manual do DPO. São Paulo: Thomson Reuters Brasil, 2021.

MARQUES, Cláudia Lima; MUCELIN, Guilherme Antônio B. **Inteligência artificial e “opacidade” no consumo:** a necessária revalorização da transparência para a proteção do consumidor. In: O direito civil na era da inteligência artificial. São Paulo: Thomson Reuters Brasil, 2020.

MARQUES, Cláudia Lima; MENDES, Laura Schertel; BERGSTEIN, Laís. Dark patterns e padrões comerciais escusos. **Revista de Direito do Consumidor**. vol. 145. ano 32. p. 295-316. São Paulo: Ed. RT, jan./fev. 2023. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/174455. Acesso em: 05 mai. 2024.

MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor. Linhas gerais de um novo direito fundamental**. Ed. Saraiva: São Paulo, 2014.

MENDES, Laura Schertel Ferreira. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. **Revista de Direito do Consumidor.** Revista dos Tribunais: São Paulo, 2015.

MENDES, Laura Schertel Ferreira. O diálogo entre o Marco Civil da Internet e o Código de Defesa do Consumidor. São Paulo: **Revista dos Tribunais**, 2016.

MENDES, Laura Schertel Ferreira. BIONI, Bruno Ricardo. O Regulamento europeu de proteção de dados pessoais e a Lei Geral de Proteção de Dados brasileira: mapeando convergências na direção de um nível de equivalência. **Revista de Direito do Consumidor**: São Paulo, 2019.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 12, n. 39, p. 185-216, 2018.

MENDES, Laura Schertel. FONSECA, Gabriel C. Soares da. STF reconhece direito fundamental à proteção de dados pessoais. **Revista de Direito do Consumidor** | vol. 130/2020 | p. 471 - 478 | Jul - Ago / 2020. Disponível em:

https://www.researchgate.net/publication/344381892_STF_reconhece_direito_fundamental_a_protecao_de_dados. Acesso em: 23 jul. 2023.

MICHAELS, Jordyn. **Pathways to the Light: Realistic Tactics to Address Dark Patterns.** Rutgers Computer and Technology Law Journal 49, n. 1: Chicago, p. 176 a 206, 2022.

MIRAGEM, Bruno. **Curso de Direito do Consumidor.** 6. ed. São Paulo: Revista dos Tribunais, 2016.

MIRAGEM, Bruno Nubens Barbosa. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor**. São Paulo: Revista dos Tribunais, 2019.

MIRAGEM, Bruno. **Curso de Direito do Consumidor**. 9. ed. Rio de Janeiro: Editora Forense, 2024.

MONTANARO, Domingo. **Medidas técnicas e administrativas para a segurança da informação**. In: Manual do DPO – Data Protection Officer. São Paulo: Revista dos Tribunais: 2021.

NARAYANAN, Arvind; MATHUR, Arunesh; CHETTY, Marshini; KSHIRSAGAR, Mihir. **Dark Patterns: Past, Present, and Future: A evolução de interfaces de usuário complicadas**. V. 18, n. 2, p. 67-92, mar./abr. 2020. Disponível em: https://doi.org/10.1145/3400899.3400901. Acesso em: 08 nov. 2024.

NUNES, Luiz Antônio Rizzato. **Comentários ao código de defesa do consumidor.** In: Minha Biblioteca, (8th edição). Grupo GEN, 2015.

PAIVA, Ana Lorena Nascimento; BISPO, Ronaldo. **Emojis, as emoções representadas graficamente no ciberespaço**. *In:* Intercom-XIX Congresso de Ciências da Comunicação na Região Nordeste. 2017.

PINTO, Carlos Alberto Mota. **Teoria Geral do Direito Civil**. 4.ed. por António Pinto Monteiro e Paulo Mota Pinto. Coimbra: Coimbra Editora, 2005.

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

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

SARLET, Ingo Wolfgang. **A EC 115/22 e a proteção de dados pessoais como Direito Fundamental**. Conjur, 2022. Disponível em: https://www.conjur.com.br/2022-mar-11/direitos-fundamentais-ec-11522-protecao-dados-pessoais-direito-fundamental. Acesso em: 29 jul. 2023.

SARMENTO, Daniel. **Direitos fundamentais e relações privadas**. 2. ed. Rio de Janeiro: Lumen Juris, 2009.

SILVA, Alexandre Assunção. A proteção pelo MPF dos dados pessoais dos usuários da internet. *In*: BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 3. **Sistema brasileiro de proteção e acesso a dados pessoais: Análise de dispositivos da Lei de acesso à informação, da Lei de identificação civil, da Lei do marco civil da internet e da Lei nacional de proteção de dados** - Brasília: MPF, 85p. - (Roteiro de Atuação; v. 3), 2019. Disponível em: http://hdl.handle.net/11549/189803. Acesso em: 28 abr. 2023.

SILVA, Lucas Gonçalves; MELO, Bricio Luis da Anunciação; KFOURI, Gustavo. A LEI GERAL DE PROTEÇÃO DE DADOS COMO INSTRUMENTO DE CONCRETIZAÇÃO DA AUTONOMIA PRIVADA EM UM MUNDO CADA VEZ MAIS TECNOLÓGICO. **Revista Jurídica**, [S.l.], v. 3, n. 56, p. 354 - 377, jul. 2019. ISSN 0103-3506. Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3581/371371972. Acesso em: 23 jul. 2023. doi:http://dx.doi.org/10.26668/revistajur.2316-753X.v3i56.3581.

SIQUEIRA, . N.; CONTIN,. C.; BARUFI,. B.; LEHFELD,. de S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD . **Revista Eletrônica Pesquiseduca**, [S. l.], v. 13, n. 29, p. 236–255, 2021. DOI: 10.58422/repesq.2021.e1029. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029. Acesso em: 20 mai. 2023.

SOUZA, Joyce; AVELINO, Rodolfo; DA SILVEIRA, Sérgio Amadeu. **A Sociedade de Controle: Manipulação e modulação nas redes sociais**. Hedra: São Paulo, 2018.

TARTUCE, Flávio; NEVES, Daniel Amorim Assumpção. **Manual de direito do consumidor**: direito material e processual. rev. e atual. Rio de Janeiro: Método, 2017.

TEPEDINO, Gustavo; SCHREIBER, Anderson. Os efeitos da Constituição em relação à Cláusula da Boa-fé no Código de Defesa do Consumidor e no Código Civil. R**evista da EMERJ**, v. 6, n. 23, Rio de Janeiro, 2003.

THE EUROPEAN DATA PROTECTION BOARD (EDPB). **Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them"**. Version 2.0. Adopted on 14 February 2023. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en.

VERBICARO, Dennis; VIEIRA, Janaína. A nova dimensão da proteção do consumidor digital diante do acesso a dados pessoais no ciberespaço. **Revista de Direito do Consumidor**: São Paulo, 2021.

VERBICARO, Dennis; RODRIGUES, Lays; ATAÍDE, Camile; Desvendando a vulnerabilidade comportamental do consumidor: uma análise jurídico-psicológica do assédio de consumo. **Revista de Direito do Consumidor**, 119. 349-384, São Paulo, 2018.

VITORELLI, Edilson. Levando os conceitos a sério: processo estrutural, processo coletivo, processo estratégico e suas diferenças. **Revista de Processo**, v. 284, p. 333-369, 2018. Disponível em: https://www.academia.edu/download/60712061/vitorelli_-_LEVANDO_OS_CONCEITOS_A_SERIO_PROCESSO_ESTRUTURAL_PROCESSO_coletivo_processo_estrategico20190926-18785-1dqvis6.pdf. Acesso em: 08 out. 2024.

XIMENES, Mariana. **O que é streaming?** Hardware.com. 2021. Disponível em: https://www.hardware.com.br/artigos/o-que-e-streaming/. Acesso em: 20 set. 2024.