



UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS JURÍDICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

JORGE MIGUEL CALANDRINI DE AZEVEDO NETO

**A PROTEÇÃO DE DADOS PESSOAIS DO CONSUMIDOR NO CIBERESPAÇO À
LUZ DA TEORIA DA CONFIANÇA: um diálogo entre o Código de Defesa do
Consumidor e a Lei Geral de Proteção de Dados Pessoais.**

BELÉM -PA
2023

JORGE MIGUEL CALANDRINI DE AZEVEDO NETO

**A PROTEÇÃO DE DADOS PESSOAIS DO CONSUMIDOR NO CIBERESPAÇO À
LUZ DA TEORIA DA CONFIANÇA: um diálogo entre o Código de Defesa do
Consumidor e a Lei Geral de Proteção de Dados Pessoais**

Dissertação apresentada à banca examinadora como requisito parcial para a obtenção do título de Mestre em Direito pelo Programa de Pós-Graduação em Direito da Universidade Federal do Pará, na Linha de Pesquisa “Direitos Fundamentais, Concretização e Garantias”, Área Temática “Consumo e cidadania”.

Orientador: Prof. Dr. Dennis Verbicaro Soares

**BELÉM-PA
2023**

**Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)**

C142p Calandrini, Jorge.
A proteção de dados pessoais do consumidor no ciberespaço à luz da teoria da confiança : um diálogo entre o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados Pessoais / Jorge Calandrini. — 2023.
180 f.

Orientador(a): Prof. Dr. Dennis Verbicaro Soares
Dissertação (Mestrado) - Universidade Federal do Pará,
Instituto de Ciências Jurídicas, Programa de Pós-Graduação em
Direito, Belém, 2023.

1. Proteção de Dados Pessoais. 2. Teoria da Confiança. 3.
Proteção do Consumidor. I. Título.

CDD 342.5

JORGE MIGUEL CALANDRINI DE AZEVEDO NETO

**A PROTEÇÃO DE DADOS PESSOAIS DO CONSUMIDOR NO CIBERESPAÇO À
LUZ DA TEORIA DA CONFIANÇA:** um diálogo entre o Código de Defesa do
Consumidor e a Lei Geral de Proteção de Dados Pessoais.

Dissertação apresentada ao Programa de Pós-graduação em
Direito do Instituto Jurídico de Ciências Jurídicas da
Universidade Federal do Pará - UFPA, como requisito
parcial para obtenção do título de Mestre. Orientador:
Prof. Dr. Dennis Verbicaro Soares.

Data do Exame: ___/___/___

Conceito:

Banca Examinadora:

Prof. Dr. Dennis Verbicaro Soares
(PPGD/UFPA – Orientador)

Prof. Dr. Ricardo Dib Taxi
(PPGD/UFPA – Avaliador Interno)

Prof. Dr. Guilherme Magalhães Martins
(PPGD/UFRRJ– Avaliador Externo)

Dedico esse feito ao meu amado filho Enrico,
minha maior motivação.

AGRADECIMENTOS

A atividade acadêmica é muito solitária, contudo, ela só é possível com uma rede de apoio. Nesse sentido, deixo meus singelos agradecimentos aos que foram importantes nessa jornada.

Ao meu filho Enrico pela sua existência. Agradeço todos os dias por estares na minha vida, sempre trazendo luz, mesmo que o céu esteja nublado e com trovoadas.

Agradeço aos meus pais, Alexandre e Paula, por todo o suporte na minha educação e nesse caminho que é o mestrado e a vida profissional. A conclusão desse objetivo só foi possível com todo apoio que recebi e recebo todos os dias. Obrigado por tudo.

Á minha vó Eliana, muito importante para o desenvolvimento da minha pesquisa, sendo uma grande financiadora do projeto, sempre fazendo o possível para que eu pudesse adquirir os livros necessários para o aprimoramento da dissertação.

Aos meus amigos, que apesar de nunca ter contado, foram importantes nos momentos de esgotamento mental e físico, ao me fazerem esquecer das dificuldades para sempre seguir em frente.

Ao meu orientador Dennis Verbicaro, que além de orientar, também, foi um professor e parceiro durante todo esse período. Obrigado.

Aos meus colegas de mestrado e do Grupo Consumo e Cidadania por todo o aprendizado nas aulas e pelas reflexões.

Gostaria de agradecer à professora Cinthia Rosa Pereira De Lima pela participação e aportes na banca de Qualificação da dissertação. Com certeza os apontamentos foram fundamentais para lapidar a ideia presente nesse trabalho e objeto de muitas reflexões.

Não há dúvida que muitas outras pessoas se fizeram presentes neste caminho e que, embora não estejam citadas, foram importantes para esse feito. Meus mais sinceros e profundos agradecimentos.

RESUMO:

O objeto é o estudo da proteção de dados sob a ótica da teoria da confiança. O objetivo geral é apresentar uma tutela de dados pessoais a partir da teoria da confiança, especialmente, no que tange a interpretação dos contratos de tratamento de dados, assim como, pela possibilidade de responsabilização em razão de frustração das legítimas expectativas do titular nos casos de vazamento de dados e desvio de finalidade do tratamento das informações pessoais. A pesquisa divide-se em quatro seções: a primeira apresenta a conjuntura da sociedade tecnológica, seus riscos e efeitos aos consumidores. A segunda investiga a evolução da matéria de proteção de dados, perpassando pelas gerações, marcos normativos até a consolidação da matéria como Direito Fundamental no ordenamento jurídico brasileiro. Assim como, dedica-se a apresentar a teoria da confiança, demonstrando seu desenvolvimento pelo Direito Privado. A terceira seção busca trazer a perspectiva da tutela dos dados pessoais alicerçada pela teoria da confiança, buscando expandir novas interpretações benéficas ao usuário vulnerável, especialmente, na valorização dos direitos de informação, transparência e responsabilização. A quarta busca apontar maneiras de tutela positiva da confiança. Neste sentido, apresenta-se os artifícios maliciosos utilizados pelas plataformas para manipular a *fides* do vulnerável e possíveis antídotos para dirimir tamanhas assimetrias. Além disso, compreende-se que para a instituição desses deveres de conduta é indispensável a atuação qualificada da Autoridade Nacional de Proteção de Dados Pessoais, apontando a necessidade de edição de uma Política Nacional de Proteção de Dados para um diálogo entre os atores do comércio eletrônico, bem como entre os órgãos e instituições de Defesa do Consumidor.

Palavras-chave: Proteção de Dados Pessoais; Teoria da Confiança; Proteção do Consumidor.

ABSTRACT

The object is the study of data protection from the perspective of trust theory. The general objective is to present a guardianship of personal data based on the theory of trust, especially with regard to the interpretation of data processing contracts, as well as the possibility of accountability due to frustration of the legitimate expectations of the holder in cases of data leakage and deviation of the purpose of the processing of personal information. The research is divided into four sections: the first presents the conjuncture of the technological society, its risks and effects to consumers. The second investigates the evolution of the data protection field, going through generations, normative milestones until the consolidation of the matter as Fundamental Law in the Brazilian legal system. As well as he dedicates himself to presenting the theory of trust, demonstrating its development by Private Law. The third section seeks to bring the perspective of the protection of personal data based on the theory of trust, seeking to expand new interpretations beneficial to the vulnerable user, especially in the valorization of information rights, transparency and accountability. The fourth seeks to point out ways of positive guardianship of trust. In this sense, the malicious devices used by the platforms to manipulate the fides of the vulnerable and possible antidotes to resolve such asymmetries are presented. In addition, it is understood that for the establishment of these duties of conduct, the qualified performance of the National Personal Data Protection Authority is indispensable, pointing out the need to edit a National Data Protection Policy for a dialogue between e-commerce actors, as well as between consumer protection agencies and institutions.

Keywords: Protection of Personal Data; Theory of Trust; Consumer Protection.

LISTA DE ABREVIATURAS E SIGLAS

- ADI- Ação Direta de Inconstitucionalidade
- ANPD- Autoridade Nacional de Proteção de Dados Pessoais
- B2C- *business to consumer*
- CC- Código Civil
- CDC- Código de Defesa do Consumidor
- CF- Constituição Federal
- CJF- Conselho da Justiça Federal
- EUA- Estados Unidos das Américas
- GDPR- *General Data Protection Regulation*
- GPS- *Global Positioning System*
- IA- Inteligência Artificial
- IBGE- Fundação Instituto Brasileiro de Geografia e Estatística
- LGPD- Lei Geral de Proteção de Dados Pessoais
- MCI- Marco Civil da Internet
- MP- Medida Provisória
- NSA – *National Security Agency*
- NSF - *National Science Foundation*
- OCDE- Organização para a Cooperação e o Desenvolvimento Econômico
- OIT - Organização Internacional do Trabalho
- OMC- Organização Mundial do Comércio
- PNAD- Pesquisa Nacional por Amostras de Domicílios
- PNRC- Política Nacional das Relações de Consumo.
- SENACON - Secretaria Nacional do Consumidor
- SNDC- Sistema Nacional de Defesa do Consumidor
- STF- Supremo Tribunal Federal
- TI - Tecnologia da Informação
- WWW- *World Wide Web*

SUMÁRIO

INTRODUÇÃO.....	11
1 SEÇÃO I- LANÇANDO LUZ SOBRE A CONJUNTURA TECNOLÓGICA	14
1.1 O surgimento da revolução tecnológica e a imersão do consumidor no ciberespaço: Plataformização, Publicidade <i>Online</i> , Capitalismo de vigilância e inteligência artificial	14
1.1.1 Do comércio eletrônico à plataformização: os seus efeitos sobre o consumidor.....	21
1.1.2 A publicidade comportamental: o assédio constante	26
1.2 A era do capitalismo de vigilância: seus impactos nos consumidores	33
1.2.1 Inteligência artificial, <i>machine learning</i> e redes convolucionais	39
1.2.2 Eficiência <i>versus</i> direitos	42
1.2.3 Exemplos de modulação algorítmica: estudos a partir do Facebook.....	43
1.2.4 A caixa preta dos algoritmos	46
1.2.5 A necessidade de adequar o direito às novas realidades sociais	52
2 SEÇÃO II- A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL E A TEORIA DA CONFIANÇA NO DIREITO PRIVADO	55
2.1 A Proteção de dados pessoais e seus fundamentos	55
2.1.1 O direito à privacidade	56
2.1.1.1 Algumas privacidades	61
2.1.1.2 Os direitos de personalidade	64
2.1.1.3 O direito à autodeterminação informativa	67
2.2 O Desenvolvimento da matéria de proteção de dados	70
2.2.1 A Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018).....	73
2.2.1.1 Fundamentos e princípios	74
2.2.1.2 Os direitos dos titulares	78
2.2.1.3 O direito à proteção de dados pessoais como um direito fundamental	80
2.3 O direito e a proteção da confiança do indivíduo nas relações contratuais	83
2.3.1 A confiança como um valor social	85
2.3.2 A confiança e o Direito Privado	89
2.3.2.1 As dimensões negativa e positiva da confiança	90
2.3.2.2 Breves notas sobre o desenvolver da teoria da confiança pelos estudos do negócio jurídico e tutela da aparência	92

2.3.2.3	A relação entre boa-fé, confiança e função social do contrato	97
2.3.2.4	O Código de Defesa do Consumidor como fonte normativa da proteção da confiança no ordenamento jurídico brasileiro	102
3	SEÇÃO III- A PROTEÇÃO DE DADOS PESSOAIS À LUZ DA TEORIA DA CONFIANÇA	108
3.1	A confiança na neutralidade das plataformas	110
3.1.1	O investimento na confiança dos consumidores pelas plataformas: desde os modelos de negócio, mecanismos de classificação e práticas publicitárias	114
3.1.2	Consentimento viciado: a tônica do ciberespaço.....	117
3.1.3	A confiança na base de tratamento do legítimo interesse.....	122
3.1.4	As legítimas expectativas dos titulares nos contratos de tratamento de dados pessoais no ciberespaço.....	127
3.2	A responsabilização civil pela frustração das legítimas expectativas do consumidor nos casos de vazamentos de dados e de desvio de finalidade do tratamento de dados	134
3.2.1	A tutela coletiva como instrumento de responsabilização das plataformas	138
3.3	SEÇÃO IV- POSSIBILIDADES DE TUTELA POSITIVA DA CONFIANÇA E A NECESSIDADE DE UMA ATUAÇÃO QUALIFICADA DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS	142
3.3.1	O conceito de racionalidade limitada e de <i>nudges</i> para economia comportamental.....	144
3.3.2	<i>Dark patterns</i> ou padrões obscuros	147
3.3.2.1	Eficácia dos padrões obscuros através de pesquisa científica randomizada	148
3.4	<i>Privacy By Design</i> e <i>Nudges</i> como Antídotos aos Padrões Obscuros	151
3.4.1	A implementação do princípio <i>privacy by design e de nudges</i>	154
4	A importância de uma atuação qualificada da autoridade nacional de proteção de dados	157
4.1	As competências da ANPD: Sancionatória educativa e fiscalizatória	157
4.2	Por uma Política Nacional de Proteção de Dados Pessoais no Brasil.....	159
	CONSIDERAÇÕES FINAIS	163
	REFERÊNCIAS	

INTRODUÇÃO

O estudo concernente a proteção de dados pessoais pelo mundo não é novo. Desde a década de 60 existe a preocupação com o controle e forma de tratamento das informações pessoais dos cidadãos. Inicialmente, essa problemática restringia-se à relação entre particular e Estado, contudo, com o desenvolvimento da *internet* essa preocupação tornou-se mais imperativa em razão da descentralização dos bancos de dados.

Neste sentido, as empresas que migraram para o comércio eletrônico começaram a ter acesso aos dados dos usuários, transformando a dinâmica existente. Se antes os dados eram concentrados na figura do Estado- O *Big Brother*, hoje as informações pessoais dos usuários estão nos bancos privados de dados dos *players*- O *Big Other*¹.

Com a posse desses dados pessoais os *players* descobriram que a navegação dos usuários na *internet* deixava informações privilegiadas sobre hábitos de consumo, e mais importante, sobre o comportamento desses indivíduos. Essa descoberta inicia uma disrupção tecnológica, emergindo um novo mercado jamais experimentado na sociedade, tornando os dados pessoais um ativo na economia da informação.

Desse modo, inicia-se o denominado capitalismo de vigilância, que se caracteriza pela busca incessante de dados pessoais sem reivindicação e tratamento dessas informações através de inteligência artificial. A corrida oriunda desse novo modelo provoca diversas violações aos direitos de privacidade e personalidade dos usuários no ciberespaço, afetando diretamente sua autodeterminação. Agravando esse cenário verifica-se que o consumidor está *hiperconfiante* nos serviços do ciberespaço, acentuando sua *hipervulnerabilidade* diante das assimetrias na relação com os *players*.

Diante desse contexto, justifica-se a presente pesquisa em três razões: uma de ordem pessoal, uma de ordem científica e outra pelo seu relevo prático e contemporâneo.

Pessoalmente, o tema de tecnologia e privacidade sempre me atraiu. O caso do *Snowden x NSA* foi um pontapé para as inquietações sobre a problemática contemporânea. Com o passar dos anos e compreendendo o valor social da privacidade para o desenvolvimento pessoal, o interesse pelo tema tornou-se um objeto de estudo.

¹ ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, [s.l.], 2015, p. 85. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754. Acesso em: 19 mar. 2022.

Sob o viés científico, a pesquisa se justifica em razão da reivindicação pelo controle dos dados pessoais ser um anseio social mundial, sendo um dos grandes problemas da sociedade tecnológica. Assim como, pela necessidade de aprofundamento de estudos sobre o fator confiança nos contratos de tratamento de dados pessoais e a sua consequente tutela pelo Direito.

No que tange a relevância prática, verifica-se que a matéria de proteção de dados no Brasil carece de maior aprofundamento, tendo em vista que a legislação geral do tema só está vigente há quase 3 anos. Desse modo, é fundamental um aprimoramento da aplicação e entendimento dessa legislação, especialmente, na ideia de proteção de legítimas expectativas dos titulares.

Não há dúvidas que o tema é central no debate acadêmico mundial, contudo, pouco foi desenvolvido em relação à confiança dos titulares nas plataformas que tratam seus dados e a necessária tutela desse valor pelo Direito.

Neste sentido, a problemática que norteia essa pesquisa pode ser compreendida a partir do seguinte questionamento: *A manipulação da confiança dos usuários pelas plataformas fragiliza a sua autodeterminação informacional nos contratos de tratamento de dados pessoais?*

Para responder o problema, a dissertação divide-se em quatro seções, cada qual correspondente a um objetivo específico: (i) Seção I- Lançando luz sobre a conjuntura tecnológica; (ii) Seção II- A proteção de dados pessoais como um direito fundamental e a teoria da confiança no direito privado; (iii) Seção III- A proteção de dados pessoais sob à luz da teoria da confiança; (iiii) Seção IV- Possibilidades de tutela positiva da confiança no ciberespaço e a necessidade de uma atuação qualificada da autoridade nacional de proteção de dados.

A primeira seção tem como objetivo identificar a conjuntura da sociedade tecnológica, abordando o início da revolução provocada pelas tecnologias da informação e comunicação. Desse modo, demonstra-se a transformação do consumo analógico para o digital, compreendendo seus riscos. Neste sentido, perpassa-se pelo movimento de plataformização da *web* até a instituição do modelo de capitalismo da vigilância. Com efeito, objetiva-se demonstrar os efeitos sobre os consumidores causados por esse modelo de capitalismo, que se constitui como uma forma de pensar e de promoção dos serviços tecnológicos, sempre pautados na extração incessante das experiências humanas para abordar os usuários dos serviços de forma personalizada.

A segunda seção, tem como objetivos específicos analisar a evolução da disciplina de proteção de dados e apresentar a teoria da confiança. Neste sentido, aborda-se sobre o desenvolvimento dos fundamentos da proteção de dados, para compreender importantes fatores históricos que impulsionaram o crescimento dos direitos ligados à dignidade da pessoa humana, como da privacidade e da personalidade. Em seguida, objetiva-se falar sobre a evolução das leis de proteção de dados pessoais, aludindo sobre suas gerações até chegar nos atuais marcos normativos, como a consolidação da proteção de dados pessoais como um direito fundamental dos cidadãos nos Estados Democráticos de Direito.

Posteriormente, expõe-se brevemente a importância do fator confiança para os sistemas sociais, com o objetivo de demonstrar o porquê da necessidade de sua tutela pelo Direito. Neste sentido, adentra-se no desenvolvimento da teoria da confiança pelo direito privado através da disciplina dos negócios jurídicos e dos contratos, demonstrando sua relação com os princípios da boa-fé e função social. Finalizando, a seção aponta o Código de Defesa do Consumidor como uma fonte normativa protetora da confiança no ordenamento jurídico brasileiro, que atuará em constante diálogo com as disposições do Código Civil, e agora, LGPD.

A terceira seção, o coração desse trabalho, propõe-se em analisar a tutela dos dados pessoais a partir da teoria da confiança. Expõe-se, inicialmente, a confiança dos usuários nas plataformas que pode ser percebida na ideia de neutralidade e nos estímulos da *fides* do vulnerável a partir dos modelos de negócio e práticas publicitárias. Em seguida, busca-se aprofundar o conceito de legítimas expectativas dos titulares nos contratos de tratamento de dados. Neste sentido, analisa-se as bases de tratamento mais utilizadas nas relações de consumo: o consentimento e o legítimo interesse. Com efeito, demonstra-se as problemáticas dessas hipóteses autorizativas diante dos arranjos do capitalismo de vigilância.

Nessa esteira, vislumbra-se a possibilidade de responsabilidade civil pela frustração das legítimas expectativas dos titulares em duas hipóteses: vazamento de dados e desvio de finalidade no tratamento das informações, apontando que a responsabilização pode ser através da via individual ou da tutela coletiva.

A quarta seção é dedicada a demonstrar as dificuldades que o usuário enfrenta ao utilizar os serviços no ciberespaço, como as *dark patterns* e intrínseca racionalidade limitada dos seres humanos. Inicialmente, apresenta-se os conceitos de racionalidade limitada e de *nudges* para depois propor a possibilidade de tutela positiva da confiança, isto é, formas de estimular deveres de informação, transparência e de boa-fé nas relações

negociais no ciberespaço. Com efeito, defende-se que o conceito de *privacy by design* e *nudges* podem atuar como antídotos para dirimir as práticas de má-fé dos *players* e da natural racionalidade limitada dos usuários, sendo possível a implementação de tais conceitos a partir da Política Nacional das Relações de Consumo- PNRC.

Neste sentido, verifica-se a fundamental importância da Autoridade Nacional de Dados Pessoais- ANPD para estimular boas práticas que assegurem transparência e autodeterminação aos usuários. Desse modo, aborda-se sobre as competências da ANPD e a possibilidade de a PRNC ser um vetor de diálogo entre os atores do comércio eletrônico, bem como dos órgãos e instituições de Defesa do consumidor. Por fim, defende-se a necessidade de uma Política Nacional de Proteção de Dados Pessoais.

Para o desenvolvimento da pesquisa foi adotado o método hipotético-dedutivo, com técnicas de pesquisa bibliográfica e legislativa. O método de abordagem utilizado se justifica, porque, de um lado, sustenta o raciocínio dedutivo de premissas derivado da pesquisa doutrinária, e, de outro, autoriza a validação das premissas, mediante indução, em casos concretos.

Pretende-se, com este trabalho, contribuir para o estado da arte do tema, enriquecendo em termos interpretativos a análise das disposições da Lei Geral de Proteção de Dados Pessoais a partir de um novo olhar, voltada para a tutela da confiança dos usuários nos contratos de tratamento de dados pessoais.

1 SEÇÃO I - LANÇANDO LUZ SOBRE A CONJUNTURA TECNOLÓGICA

Diz-se que a luz do sol é o melhor dos desinfetantes
Louis Brandeis²

1.1 O surgimento da revolução tecnológica e a imersão do consumidor no ciberespaço: plataformação, publicidade *online*, capitalismo de vigilância e inteligência artificial

A produção inventiva de novas tecnologias acompanha a trajetória humana, auxiliando na promoção do progresso e do desenvolvimento³. Algumas dessas inovações técnicas

² No original: “Sunlight is said to be the best of disinfectants” (BRANDEIS, Louis D. What Publicity Can Do. *Harper’s Weekly*, USA, December 20, 1913, p. 10. Disponível em: http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1910/1913_12_20_What_Publicity_Ca.pdf. Acesso em: 29 mar. 2022).

³ CASTELLS, Manuel. *Sociedade em rede*. Tradução de Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 1998. v. 1, p. 45.

causaram revoluções na sociedade em seu período, como a criação da roda, da máquina a vapor, do telefone e agora as tecnologias da informação.

Antes de examinar o atual estágio, marcado pela alta complexidade tecnológica, pela utilização maciça da inteligência artificial (IA), pela perda de privacidade e pelos riscos para a personalidade dos indivíduos, é necessário abordar o começo da revolução tecnológica para entender como se chegou às caixas pretas que, em grande proporção, nos dominam.

As tecnologias da informação representam uma nova virada de Copérnico para a sociedade, penetrando na comunidade e gerando mudanças nas estruturas sociais, econômicas e culturais⁴. Emerge assim um modelo em que a competitividade e a produção são centradas na informação, decorrente da geração de conhecimentos. Embora o conhecimento e a informação sempre tenham sido essenciais nos modelos de desenvolvimento anteriores, as tecnologias da informação tornaram esses signos a principal fonte de produtividade⁵, e os mercados orientam-se por esses dados de conhecimento.

Para Castells, a revolução provocada pelas tecnologias da informação criou um modelo de orientação do desenvolvimento da sociedade, dando origem à era do informacionalismo. Desse modo, a produção e a competitividade lastreiam-se nas informações e nos conhecimentos obtidos pelas tecnologias. Por isso, o sociólogo defende que se vive em um *capitalismo informacional*. Em sua visão, esse capitalismo seria uma *perestroika* do modelo econômico de produção perpetuado, pois o modelo keynesiano de crescimento capitalista atingiu “as suas próprias limitações no início da década de 1970, e a sua crise manifestou-se sob a forma de inflação desenfreada”⁶. Assim, o novo paradigma tecnológico permitiu uma reconstrução do modelo de produção, possibilitando, para o autor, “a expansão e o rejuvenescimento do capitalismo, como o industrialismo estava ligado à sua constituição como modo de produção”⁷.

O capitalismo informacional, organizado em torno das tecnologias da informação, é flexível e adaptável, mas distingue-se dos demais porque nele a informação tornou-se *a própria mercadoria do processo produtivo*⁸. Dessa maneira, a informação é a matéria-prima do novo paradigma tecnológico; como a informação é o ponto central desse modelo, o capitalismo informacional é dinâmico, possuindo a capacidade de tornar seus processos reversíveis e de

⁴ LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999, p. 17. Quanto ao neologismo “cibercultura”, desina aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço.

⁵ CASTELLS, *loc. cit.*, p. 53-54.

⁶ *Ibid.*, p. 55.

⁷ CASTELLS, *loc. cit.*

⁸ *Ibid.*, p. 119.

modificar os modelos das instituições⁹. Com efeito, a economia da informação digitalizou os dados em átomo (papel) na forma de *bits*, tecnologia possível por meio do sistema binário (1 e 0) de dígitos. Assim, os computadores passaram a processar e a armazenar as informações em grande escala¹⁰. Esse avanço tecnológico apresenta benefícios, como a capacidade de coletar e de armazenar dados como nunca, bem como a proteção dessas informações de maneira muito mais segura do que no modo analógico¹¹.

Em razão dos avanços tecnológicos, entende-se que o final do século XX é um dos raros intervalos na história de transformações das estruturas sociais, sendo um evento histórico da mesma importância da Revolução Industrial do século XVIII, por ter induzido uma descontinuidade nas bases materiais da economia, da sociedade e da cultura. Nesse sentido, as revoluções tecnológicas ao longo da história têm como característica a sua penetrabilidade na sociedade, isto é, inserem-se em todos os domínios da vida humana¹², o que é percebido com a difusão, a consolidação e até a dependência das tecnologias da informação no dia a dia da contemporaneidade.

Para que fosse possível a sociedade em redes, a criação e o desenvolvimento da *Internet* foram fundamentais para a penetrabilidade das tecnologias da informação na comunidade global. O nascimento dessa tecnologia primordial para o capitalismo informacional foi gestado por diferentes atores, passando pelos setores militares, pela cooperação científica entre pesquisadores e adeptos da contracultura. A *Internet* foi fruto da Agência de Projetos de Pesquisa Avançada – em inglês, *Advanced Research Projects Agency* – do Departamento de Defesa dos Estados Unidos, e seu objetivo era ser um sistema de comunicação invulnerável a ataques nucleares. Em 1969, a primeira rede de computadores iniciou seu funcionamento. Denominada *Arpanet*, seus usuários eram militares e universidades norte-americanas¹³. Dessa

⁹ *Ibid.*, p. 109.

¹⁰ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 6.

¹¹ “As informações codificadas digitalmente podem ser transmitidas e copiadas quase indefinidamente *sem perda de informação*, já que a mensagem pode ser quase sempre reconstituída integralmente apesar das degradações causadas pela transmissão (telefônica, hertziana) ou pela cópia. O que não é, evidentemente, o caso dos sons e das imagens gravados de forma analógica, os quais se degradam irremediavelmente a cada nova cópia” (LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999, p. 51, grifo nosso).

¹² CASTELLS, *loc. cit.*, p. 68.

¹³ “A primeira rede de computadores, que se chamava ARPANET – em homenagem a seu poderoso patrocinador – entrou em funcionamento em 1.º de setembro de 1969, com seus quatro primeiros nós na Universidade da Califórnia em Los Angeles, no Stanford Research Institute, na Universidade da Califórnia em Santa Bárbara e na Universidade de Utah. Estava aberta aos centros de pesquisa que colaboravam com o Departamento de Defesa dos EUA, mas os cientistas começaram a usá-la para suas próprias comunicações, chegando a criar uma rede de mensagens entre entusiastas de ficção científica. A certa altura tornou-se difícil separar a pesquisa voltada para fins militares das comunicações científicas e das conversas pessoais. Assim, permitiu-se o acesso à rede de cientistas de todas as disciplinas e, em 1983, houve a divisão entre ARPANET, dedicada a fins científicos e a

maneira, a rede desenvolveu-se entre os setores acadêmicos e militares, até que, em 1980, criou-se a *Arpa-Internet*, que posteriormente passou a se chamar *Internet*. Ressalta-se que o desenvolvimento da *Internet* ocorreu sob a supervisão estatal, sendo a *National Science Foundation* (NSF) dos EUA o último órgão do Estado a operar a espinha dorsal da *Internet* até a inevitável privatização da rede¹⁴.

A *Internet*, desde seu início, gerou um ambiente de novas possibilidades para inovações tecnológicas. Esse ambiente de novidades e descobertas estava em sintonia com o contexto social, político e cultural dos anos 70 do século XX e encontrou um entorno de vultosos fundos de financiamento do Departamento de Defesa dos EUA para o fomento de novas tecnologias. É nessa conjuntura que nasce o Vale do Silício, na Califórnia. Ressalta-se que, além da importância dos investimentos, o movimento (contra)cultural eferescente na Califórnia foi determinante para inspirar inovações científicas. Assim, com o domínio das novas técnicas e com novos pensamentos culturais, houve a criação de tecnologias que mudariam a sociedade, como os computadores pessoais¹⁵. Em 1975, a *Apple* colocou o primeiro computador pessoal no mercado e, em 1977, o *Apple II* foi um sucesso comercial¹⁶.

Observa-se que a *Internet* foi o resultado de um conjunto de diferentes conjunturas, entre as quais estavam objetivos militares, a ideia de uma rede de cooperação científica entre pesquisadores e um movimento social pujante que criaram as bases da sociedade hiperconectada atual. Contudo, a criação da sociedade em rede como se conhece na atualidade é oriunda da década de 90, momento da privatização da *Internet*. Dessa maneira, diversas empresas e corporações começaram a navegar no denominado *World Wide Web* (WWW). Após a padronização de protocolos e a criação da WWW, foi possível a organização dos *sites* por informação, e não por localização. Assim ocorreu a uniformização de endereços eletrônicos com o *uniform resource locator* (URL)¹⁷.

A partir do desenvolvimento da *Internet* e das inovações tecnológicas do Vale do Silício, foi possível a consolidação da sociedade global conectada e desterritorializada. Com efeito, o

MILNET, orientada diretamente às aplicações militares” (CASTELLS, Manuel. *Sociedade em rede*. Tradução de Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 1998. v. 1, p. 82-83).

¹⁴ “Contudo, as pressões comerciais, o crescimento de redes de empresas privadas e de redes cooperativas sem fins lucrativos levaram ao encerramento dessa última espinha dorsal operada pelo governo em abril de 1995, renunciando a privatização total da Internet, quando inúmeras ramificações comerciais das redes regionais da NSF uniram forças para formar acordos colaborativos entre redes privadas” (*Ibid.*, p. 83).

¹⁵ É o que entendem os autores já citados: LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999, p. 31; CASTELLS, Manuel. *Sociedade em rede*. Tradução de Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 1998. v. 1, p. 82 *et seq.*

¹⁶ CASTELLS, *loc. cit.*, p. 91.

¹⁷ *Ibid.*, p. 88.

novo estágio do capitalismo caracteriza-se por ser informacional, global e em rede¹⁸. As cadeias produtivas e de distribuição dos produtos estão em diversos países do globo. Um exemplo é a empresa de material esportivo *Nike*, que possui cadeias de distribuição nos Estados Unidos, na Holanda, na Bélgica, na China e em outros países¹⁹, além de fábricas no Vietnã e na China²⁰.

Nessa esteira, *Facebook Inc.*, *Alphabet Inc.* e *Twitter*, por exemplo, empregam seus moderadores de conteúdo em vários pontos do globo, havendo a terceirização desse serviço principalmente no Sudeste Asiático²¹. Portanto, as cadeias de produção, de distribuição e o mercado de consumo passam a ser globais, mesmo para empresas de tecnologia ou de varejo.

Em decorrência da sociedade em redes, as empresas migraram para a *internet*, expandindo seus mercados consumidores e criando um espaço onde as pessoas de qualquer lugar do mundo poderiam interagir e consumir em um ambiente denominado “ciberespaço”, que Pierre Lévy assim define:

é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo²².

O termo “ciberespaço” é utilizado há décadas. Luciano Floridi, filósofo de ética da informação da Universidade de Oxford, retoma o termo, mas entende que no atual momento

¹⁸ “É *informacional* porque a produtividade e a competitividade de unidades ou agentes nessa economia (sejam empresas, regiões ou nações) dependem basicamente de sua capacidade de gerar, processar e aplicar de forma eficiente a informação baseada em conhecimentos. É *global* porque as principais atividades produtivas, o consumo e a circulação, assim como seus componentes (capital, trabalho, matéria-prima, administração, informação, tecnologia e mercados) estão organizados em escala global, diretamente ou mediante uma rede de conexões entre agentes econômicos. É *rede* porque, nas novas condições históricas, a produtividade é gerada, e a concorrência é feita em uma rede global de interação entre redes empresariais” (*Ibid.*, p. 119, grifo do autor).

¹⁹ É o que consta no *site* da empresa: “Para garantir que realizemos nossos compromissos com o consumidor, as equipes da cadeia de suprimentos trabalham com uma rede de mais de 50 centros de distribuição, milhares de clientes e mais de 100 mil lojas de varejo no mundo todo, tornando o impossível possível todos os dias” (CENTROS de distribuição da Nike. *Nike Careers*, [202-]. <https://jobs.nike.com/pt/distributioncenters>. Acesso em: 8 mar. 2022).

²⁰ “De acuerdo con la funcionaria, 88 del total de 112 fábricas de Nike están ubicadas en la región sureste de Vietnam y se encargan de la producción de *zapatillas* de la marca Nike (RECHAZAN información sobre el traslado de Nike de sus fábricas de Vietnam. *Vietnam Plus*, 5 out. 2021. Disponível em: <https://es.vietnamplus.vn/rechazan-informacion-sobre-el-traslado-de-nike-de-sus-fabricas-de-vietnam/142024.vnp>. Acesso em: 8 mar. 2022).

²¹ “Atualmente, o Sudeste Asiático é a principal escolha de empresas como Facebook Inc., Alphabet Inc. (principalmente para o Youtube) e Twitter para terceirizar esse tipo de serviço. O fato de países como a Índia e as Filipinas terem sido colonizados por nações de língua inglesa, com a cultura do Reino Unido e dos Estados Unidos impostas na educação e no entretenimento como parte desse processo, é visto como um atrativo para as *big techs* escolherem essas regiões para terceirizar parte de suas operações” (MACHADO, Débora Franco. A colonização dos dados como produto das operações das mídias sociais no sul global. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021, p. 56-57).

²² LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999, p. 17.

não há mais ambientes separados, como denota o termo *ciber*²³. Na realidade, existe uma confusão entre o mundo digital e o analógico no dia a dia dos cidadãos. Por isso, na visão do autor, há uma *infosfera*, termo que “ajuda a definir o ambiente em que vivemos, feito de informações, fluxos de dados, interações com softwares e sistemas automáticos, em um misto de analógico e digital, e assim por diante”²⁴.

Apesar de concordarmos com a confusão entre o mundo analógico e o digital identificado por Fiordi, adotamos, no desenvolvimento deste trabalho, o termo “ciberespaço”, porque a análise proposta limita-se às relações consumeristas na *internet*. Como explica Floridi, *ciber* designa um ambiente separado, apenas relacionado com o digital, o que está em conformidade com a análise objeto desta pesquisa.

Com o desenvolvimento do ciberespaço, as empresas do Vale do Silício começam a dominar o mercado tecnológico, muito em razão do *know-how* adquirido no início da revolução tecnológica. Assim, as principais empresas estabelecidas na atualidade iniciaram suas operações e revolucionaram com novos serviços²⁵.

Uma das criações disruptivas²⁶ do Vale do Silício foi o *e-commerce*, que inaugurou uma transformação nas relações de consumo, criando um mercado para os consumidores no mundo

²³ “O termo [infosfera] circula há algum tempo. Eu o recuperei filosoficamente para falar de duas coisas. Por um lado, ele nos ajuda a definir o ambiente em que vivemos, feito de informações, fluxos de dados, interações com softwares e sistemas automáticos, em um misto de analógico e digital, e assim por diante. Nesse sentido, é uma atualização do velho termo ‘ciberespaço’. Aqui a utilidade está em abandonar a ideia de que há espaços separados, como se a infosfera fosse um lugar quase alheio, diferente, inatural, isto é, ‘ciber’, no qual entramos e saímos como e quando queremos. Na realidade, a infosfera é o habitat cotidiano para bilhões de pessoas, cada vez mais, e cada vez mais comumente. Por outro lado, eu usei o termo ‘infosfera’ ontologicamente, para falar da realidade em geral, em uma metafísica que interpreta o Ser de modo informacional. Se, de um ponto de vista informacional, tudo pode ser lido como feito de informação (pensemos no estruturalismo ou na filosofia da ciência), então ‘infosfera’ e ‘Ser’ se tornam correferenciais” (FLORIDI, Luciano. Ser humano e inteligência artificial: os próximos desafios do onlife. Entrevista concedida a Gian Paolo Terravecchia. Tradução de Moisés Sbardelotto. *Instituto Humanitas Unisinos*, 28 out. 2020, grifo do autor. Disponível em: www.ihu.unisinos.br/78-noticias/604136-ser-humano-e-inteligencia-artificial-os-proximos-desafios-do-onlife-entrevista-com-luciano-floridi. Acesso em: 11 mar. 2021).

²⁴ FLORIDI, *loc. cit.*

²⁵ “Na década de 1990, quando a internet foi privatizada e se tornou tecnologia comercial, o Vale do Silício também conseguiu capturar o novo ramo de atividades. As principais empresas de equipamento para a Internet (como a Cisco Systems), empresas de implantação redes computadores (como a Sun Microsystems), empresas de *software* (como a Oracle), e portais da Internet (como o Yahoo!) começaram no Vale do Silício. Ademais, a maioria das empresas novatas da internet que inauguraram o *e-commerce* e revolucionaram o comércio (como o Ebay), também estavam agrupadas no Vale do Silício” (CASTELLS, Manuel. *Sociedade em rede*. Tradução de Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 1998. v. 1, p. 103).

²⁶ “First, a quick recap of the idea: ‘Disruption’ describes a process whereby a smaller company with fewer resources is able to successfully challenge established incumbent businesses. Specifically, as incumbents focus on improving their products and services for their most demanding (and usually most profitable) customers, they exceed the needs of some segments and ignore the needs of others. Entrants that prove disruptive begin by successfully targeting those overlooked segments, gaining a foothold by delivering more-suitable functionality – frequently at a lower price. Incumbents, chasing higher profitability in more-demanding segments, tend not to respond vigorously. Entrants then move upmarket, delivering the performance that incumbents’ mainstream customers require, while preserving the advantages that drove their early success. When mainstream customers

digital. Com o desenvolvimento do comércio eletrônico, os consumidores começaram a migrar do consumo analógico para o digital, intensificando o processo de imersão do consumidor no ciberespaço.

No cenário mundial, as empresas baseadas nas tecnologias da informação superaram em pouco tempo as principais empresas do mundo de diversos setores empresariais, como o automobilístico, o empreiteiro, o varejista e outros. As empresas de tecnologia *Apple* e a *Amazon* estão entre as 10 maiores empresas do mundo, ao lado de bancos e de grandes conglomerados²⁷. O *Facebook* está perto de alcançar a marca de 3 bilhões de usuários ativos, o que corresponde a praticamente 35% da população mundial²⁸.

Segundo o Instituto Brasileiro de Geografia e Estatística, atualmente no Brasil 82,7% dos domicílios brasileiros têm acesso à *internet*²⁹. De cada quatro brasileiros, três têm acesso à *internet*, totalizando 134 milhões de usuários. Desse montante, 90% acessam a rede todos os dias, principalmente por meio de *smartphones*³⁰. Estima-se que o comércio eletrônico de produtos tenha cerca de 41 milhões de consumidores ativos no país³¹. A empresa Accenture, gigante global de *marketing*, após ser contratada pela Meta (*holding* do *Facebook*), em 2020, divulgou que 83% dos consumidores brasileiros utilizam o aplicativo *WhatsApp* para consumir produtos e serviços³².

start adopting the entrants' offerings in volume, disruption has occurred" (CHRISTENSEN, Clayton; RAYNOR, Michael E.; MCDONALD, Rory. What is Disruptive Innovation? *Harvard Business Review Magazine*, Dec. 2015. Disponível em: <https://hbr.org/2015/12/what-is-disruptive-innovation>. Acesso em: 8 mar. 2022).

²⁷ MURPHY, Andrea; HAVERSTOCK, Elisa; GARA, Antoine; HELMAN, Chris; VARDI, Nathan. Global 2000: as maiores empresas de capital aberto do mundo em 2021. *Forbes*, 13 maio 2021. Disponível em: <https://forbes.com.br/forbes-money/2021/05/global-2000-as-maiores-empresas-de-capital-aberto-do-mundo-em-2021/>. Acesso em: 30 set. 2021.

²⁸ VITORIO, Tamires. Facebook fica mais perto de 3 bilhões de usuários ativos e receita cresce em 2020. *EXAME*, São Paulo, 28 jan. 2021. Disponível em: <https://exame.com/invest/facebook-fica-mais-perto-de-3-bilhoes-de-usuarios-ativos-e-receita-cresce-em-2020/amp/>. Acesso em: 30 set. 2021.

²⁹ A população brasileira está cada vez mais conectada. É o que mostra a Pesquisa Nacional por Amostra de Domicílios (PNAD) de 2019, realizada pelo IBGE. "De acordo com o levantamento, 82,7% dos domicílios nacionais têm acesso à internet, um aumento de 3,6 pontos percentuais em relação a 2018" (PESQUISA mostra que 82,7% dos domicílios brasileiros têm acesso à internet. *Ministério das Comunicações*, 14 abr. 2021. Disponível em: [https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet#:~:text=IBGE-,%20Pesquisa%20mostra%20que%2082%2C7%25%20dos%20domic%20C%ADlios,brasileiros%20t%20C%AAm%20acesso%20%20C%20internet&text=A%20popula%20C%20A3o%20brasileira%20est%20C%20A1%20cada,Geografia%20e%20Estat%20C%ADstica%20\(IBGE\)](https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet#:~:text=IBGE-,%20Pesquisa%20mostra%20que%2082%2C7%25%20dos%20domic%20C%ADlios,brasileiros%20t%20C%AAm%20acesso%20%20C%20internet&text=A%20popula%20C%20A3o%20brasileira%20est%20C%20A1%20cada,Geografia%20e%20Estat%20C%ADstica%20(IBGE).). Acesso em: 18 mar. 2022).

³⁰ VALENTE, Jonas. Brasil tem 134 milhões de usuários de internet, aponta pesquisa. *Agência Brasil*, 26 maio de 2022. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa>. Acesso em: 8 mar. 2022.

³¹ INGIZZA, Carolina. Vendas online no Brasil crescem 47% no 1º semestre, maior alta em 20 anos. *EXAME*, 27 ago. 2020. Disponível em: <https://exame.com/pme/e-commerce-brasil-cresce-47-primeiro-semester-alta-20-anos/>. Acesso em: 8 mar. 2022.

³² PRADO, Filipe. Comércio social deve movimentar US\$ 1,2 trilhão em 2025, indica pesquisa. *Istoé Dinheiro*, 11 jna. 2022. São Paulo. Disponível em: <https://www.istoedinheiro.com.br/comercio-social-deve-movimentar-u-12-trilhao-em-2025-indica-pesquisa/>. Acesso em: 14 mar. 2022.

Pelos dados expostos, constata-se a imersão da comunidade global no ciberespaço. Com o consumidor brasileiro, não poderia ser diferente: está cada vez mais hiperconectado para adquirir produtos e serviços. Mas não se pode olvidar que a pandemia da covid-19 foi fundamental para uma inserção abrupta de vários consumidores no Brasil e no mundo, sendo um fator importante no processo de imersão tecnológica dos usuários³³.

Nota-se como a revolução tecnológica gerou uma tendência de virtualização das relações humanas. O capitalismo informacional, que tem como base a *internet*, as tecnologias da informação e a globalização, impulsionou essa tendência, como pode ser observado nas relações de consumo. Nesse sentido, verifica-se como os consumidores estão cada vez mais hiperconectados, realizando interações sociais e transações econômicas todos os dias no ciberespaço.

Segundo Rodotà, o ciberespaço incentivou “um lugar asséptico, onde o consumidor, adulto ou criança, pode entrar como em um imenso *shopping center*, sem correr o risco de ser incomodado por qualquer coisa que possa afastá-lo da simples atividade do consumo”³⁴. Essa mudança econômica e social está causando um processo constante de imersão tecnológica do consumo. Por isso, faz-se necessário demonstrar as transformações decorrentes do comércio eletrônico e os riscos para a proteção de dados dos consumidores nesse ambiente.

1.1.1 Do comércio eletrônico à plataformação: efeitos no consumidor

Assim como a criação das marcas³⁵, o comércio eletrônico representa uma transformação paradigmática na forma de consumir, com inovações que modificaram a sociedade do consumo.

³³ “O comércio eletrônico foi, sem dúvidas, um dos setores que mais cresceu durante a pandemia. Nesses últimos dois anos, milhões de pessoas que, até então nunca tinham feito um único pedido online, tiveram a primeira experiência de comprar um produto ou pedir uma refeição pela internet. Apenas 5% de todo varejo brasileiro realizava vendas por meios digitais até o surgimento da Covid-19 e a expectativa é que esse número pelo menos dobre até o final do ano de 2021” (MAGNANI, Vitor. Físico e Digital: O futuro do comércio é “online to offline”. *Forbes*, 21 out. 2021. Brasil. Disponível em: <https://forbes.com.br/forbes-tech/2021/10/fisico-e-digital-o-futuro-do-comercio-e-online-to-offline/#:~:text=Apenas%205%25%20de%20todo%20varejo,final%20do%20ano%20de%202021>. Acesso em: 8 mar. 2022).

³⁴ RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 158.

³⁵ “O aparecimento das grandes marcas e dos produtos acondicionados transformou profundamente a relação do consumidor com o varejista, este perdendo as funções que até então lhe estavam reservadas: daí em diante, não é mais no vendedor que se fia o consumidor, mas na marca, sendo a garantia e a qualidade dos produtos transferidas para o fabricante. Rompendo a antiga relação mercantil dominada pelo comerciante, a fase I transformou o cliente tradicional em consumidor moderno, em consumidor de marcas a ser educado e seduzido

A Organização Mundial do Comércio (OMC) define o comércio eletrônico como a “produção, distribuição, *marketing*, venda e entrega de bens e serviços por meios eletrônicos entre empresas, indivíduos, governos e outras organizações”; de acordo com a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), o *e-commerce* são “transações realizadas digitalmente de bens e serviços que podem ser entregues digitalmente ou fisicamente e que envolvem consumidores, firmas e governos”³⁶.

As mudanças promovidas pelo comércio digital em comparação com o analógico são evidentes, pois, no consumo analógico, o consumidor deve dirigir-se a um empreendimento físico, no qual terá a sua disposição um vendedor que poderá tirar suas dúvidas sobre o produto, como sua composição, suas funções e sua maneabilidade. Nesse contexto, o consumidor possui uma limitação física, isto é, somente comprará de empreendimentos localizados na região em que mora, pois é mais complicado conseguir comprar produtos de lojas em outra cidade, por exemplo. Já no comércio eletrônico, o consumidor pode entrar e sair de diferentes fornecedores, de diferentes estados ou países sem a necessidade de se locomover. Embora não possua o auxílio do vendedor para conhecer melhor o produto, a comodidade e a rapidez fizeram com que esse método de consumo fosse incorporado aos hábitos da sociedade. Além disso, no *e-commerce* é possível adquirir serviços, *softwares*, aplicativos, músicas e arquivos digitais intangíveis.

O comércio eletrônico caracteriza-se pela despersonalização, pela desterritorialização e pela desmaterialização³⁷. Sendo assim, não há vendedor; as relações são, então, despersonalizadas e assíncronas; o consumo é livre de barreiras geográficas, sendo, portanto, desterritorializado; o consumo é desmaterializado, pois é possível adquirir produtos intangíveis.

Sendo assim, o *business to consumers* (B2C) é uma realidade desafiadora para a ciência jurídica³⁸, ainda mais com o agravamento incitado pelas novas práticas e tecnologias de coleta e de tratamento de dados dos consumidores promovidas pelas plataformas. Embora o termo

especialmente pela publicidade” (LIPOVETSKY, Gilles. *A felicidade paradoxal: ensaio sobre a sociedade de hiperconsumo*. São Paulo: Companhia das Letras, 2007, p. 29-30).

³⁶ COMÉRCIO eletrônico. *Gov.br*, Ministério das Relações Exteriores, 7 jul. 2020. Disponível em: <https://www.gov.br/mre/pt-br/assuntos/politica-externa-comercial-e-economica/comercio-internacional/comercio-eletronico#:~:text=A%20Organiza%C3%A7%C3%A3o%20Mundial%20do%20Com%C3%A9rcio%20e%20que%20envolvem%20consumidores%20e%20governos%E2%80%9D>. Acesso em: 15 mar. 2022.

³⁷ MARQUES, Claudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*. São Paulo: Revista dos Tribunais, 2004, p. 63 *et seq.*

³⁸ MARQUES, Claudia Lima. Proteção do consumidor no comércio eletrônico e a chamada nova crise do contrato: por um direito do consumidor aprofundado. *Revista de Direito do Consumidor*, São Paulo, v. 15, n. 57, jan./mar. 2006, p. 23.

plataforma denote abertura, essas são, na realidade, fechadas, trata-se de uma metáfora, segundo Gillespie³⁹.

O conceito de plataforma é multifacetado, sendo adotado em diversas áreas do conhecimento⁴⁰, mas há um certo consenso no sentido de que plataforma é um mercado de dois ou mais lados⁴¹. Desse modo, “o termo plataforma deve ser visto como ‘produtivo’ por si só, levando os usuários a organizar suas atividades em torno de plataformas proprietárias e com fins lucrativos”⁴². Poell, Nieborg e Van Dijck definem plataforma “como infraestruturas digitais (re)programáveis que facilitam e moldam interações personalizadas entre usuários finais e complementadores, organizadas por meio de coleta sistemática, processamento algorítmico, monetização e circulação de dados”⁴³.

A proliferação de plataformas no ciberespaço foi possível por meio da chamada *Web 2.0*. Com a *Web 2.0*, a *internet* tornou-se uma plataforma para usuários e empresas⁴⁴. Dessa

³⁹ “Figuratively, a platform is flat, open, sturdy. In its connotations, a platform offers the opportunity to act, connect, or speak in ways that are powerful and effective: catching the train, drilling for oil, proclaiming one’s beliefs” (GILLESPIE, Tarleton. The Platform Metaphor, Revisited. *Digital Society Blog*, 24 Aug. 2017. Disponível em: <https://www.hiig.de/en/the-platform-metaphor-revisited/>. Acesso em: 15 mar. 2022).

⁴⁰ “O uso do conceito de plataforma, tanto na academia quanto no mercado, sofreu várias mudanças importantes desde o início do novo milênio. Antecedendo a chegada dos atuais gigantes da tecnologia, como Google e Facebook, os campos de economia (de redes) e estudos na área de negócios já popularizavam e teorizavam sobre o termo plataforma, com maior destaque para Japão, França e Estados Unidos [...]. No início dos anos 2000, empresas americanas como Microsoft, Intel e Cisco forneceram a pesquisadores da área de administração alguns exemplos ricos de como alcançar a ‘liderança da plataforma’ [...]. Uma das contribuições mais influentes conceituou plataformas (por exemplo, consoles de videogames) como ‘mercados de dois lados’ [...]. Os operadores da plataforma, neste caso, agregam, por um lado, compradores ou usuários finais (por exemplo, jogadores) e, por outro, vendedores ou editores de jogos. As contribuições teóricas posteriores incorporaram trabalhos de áreas vizinhas, como economia de organização industrial, gerenciamento estratégico e tecnologia da informação. Isso teve um impacto significativo no discurso e nas estratégias de negócios implementados pelas empresas de plataformas, muito mais do que as perspectivas críticas em relação à mídia. Na pesquisa em comunicação, a emergência do conceito de plataforma evoluiu ao lado de discussões sobre mudanças mais amplas nas tecnologias da comunicação, na economia da informação e na subsequente reorientação dos usuários como produtores ativos de cultura [...]” (POELL, Thomas; NIEBORG, David; VAN DIJCK, José. Plataformização. *Revista Fronteiras: estudos midiáticos*, Porto Alegre, v. 22, n. 1, jan./abr. 2020, p. 3. Disponível em: https://www.researchgate.net/publication/341921979_Plataformizacao. Acesso em 09 Fev 2023).

⁴¹ “Embora a pesquisa em negócios e os estudos de software tenham compreensões diferentes sobre plataformas, essas perspectivas se complementam efetivamente: interesses e esforços de negócios para desenvolver mercados de dois lados auxiliam no desenvolvimento de infraestruturas de plataformas. As arquiteturas das plataformas são modulares em seu design, de modo que a tecnologia pode ser aberta seletivamente a complementadores para criar a integrar seus serviços a serem usados pelos usuários finais. Para obter uma visão das plataformas como mercados e infraestruturas computacionais, é vital combinar essas abordagens” (*Ibid.*, p. 3-4).

⁴² *Ibid.*, p. 3.

⁴³ *Ibid.*, p. 4.

⁴⁴ “Em 2004, reconheceu-se que os serviços como Del.icio.us, a Wikipedia e o MySpace foram os representativos da entrada em uma nova era comportamental da Internet, quando o modo unidirecional de criação de conteúdo começou a ser modificado para o modo bidirecional, ou seja, não mais o conteúdo era apenas exposto e acessado pelos usuários, senão também eles o criaram, conformando a “*read/write Web*”, em contraponto à “*read-Only Web*” [`javascript:void\(0\)`](https://www.javascript:void(0)). O’Reilly chama esse período, que compreenderia os anos de 2000 a 2010, de *Web 2.0* ou *Social Web* e a descreve como um novo estágio na evolução da Internet que se configura como uma plataforma mundial que conecta pessoas e que possibilita novas experiências aos usuários por meio de interfaces simplificadas, que se tornaram disponíveis para computadores pessoais” (MUCELIN, Guilherme. *Conexão*

maneira, a *internet* transformou-se em um espaço de colaboração e de participação entre os seus usuários, sendo chamada *the participatory web*⁴⁵. A rede passa, então, de um meio de apenas publicações de informações para uma infraestrutura que permite a criação de serviços de *software* e a participação dos usuários⁴⁶.

Caminha-se, portanto, para um processo de “plataformização”⁴⁷ do ciberespaço, onde os fornecedores desenvolvem seus programas baseados em coleta de dados e inteligência artificial para operar seus modelos de negócios. Anne Helmond explica que o termo plataformização “refere-se à plataforma como o modelo econômico e de infraestrutura dominante na rede social. Menciona ainda as consequências da expansão das plataformas de mídia social em outros espaços *online* ⁴⁸”. Com efeito, a plataformização possui três dimensões: infraestrutura de dados⁴⁹, mercado⁵⁰ e governança⁵¹.

online e hiperconfiança: os players da economia do compartilhamento e o direito do consumidor. São Paulo: Revista dos Tribunais, 2020. *E-book*. cap. 1).

⁴⁵ “[...] Matthew Allen (2013) argues, we should see Web 2.0 as ‘rhetorical technology’ in which ‘the computing industry attempted to change the way we think of the internet’ (p. 264), from publishing channel to software development platform” (HELMOND, Anne. The Platformization of the Web: Making Web Data Platform Ready. *Social Media + Society*, Sept. 30, 2015. Disponível em: <https://journals.sagepub.com/doi/10.1177/2056305115603080>. Acesso em: 15 mar. 2022).

⁴⁶ *Ibid.*, p. 3.

⁴⁷ “Seguindo pesquisas em estudos de software, na área de negócios e na economia política, compreendemos plataformização como a penetração de infraestruturas, processos econômicos e estruturas governamentais de plataformas em diferentes setores econômicos e esferas da vida” (POELL; NIEBORG; VAN DIJCK, *loc. cit.*, p. 5).

⁴⁸ To refer to the rise of the platform as the dominant infrastructural and economic model of the social web and the consequences of the expansion of social media platforms into other spaces online (HELMOND, Anne. The Platformization of the Web: Making Web Data Platform Ready. *Social Media + Society*, Sept. 30, 2015. Disponível em: <https://journals.sagepub.com/doi/10.1177/2056305115603080>. Acesso em: 15 mar. 2022.)

⁴⁹ A primeira dimensão é o desenvolvimento de infraestruturas de dados, que tem sido explorado especialmente pelos estudos de *software*. Como processo, o desenvolvimento de infraestruturas de dados tem sido apreendido por meio da noção de dataficação, que se refere às maneiras pelas quais as plataformas digitais se transformam em dados, práticas e processos que historicamente escaparam à quantificação. Esse processo não se refere apenas a dados demográficos ou a dados de perfil oferecidos pelos usuários ou solicitados por meio de pesquisas *online*, mas principalmente a metadados comportamentais. Essa coleta de dados comportamentais é proporcionada pela expansão de infraestruturas das plataformas na forma de aplicativos, *plug-ins*, rastreadores e sensores ativos e passivos (*Ibid.*, tradução nossa).

⁵⁰ A segunda dimensão da plataformização diz respeito aos mercados, à reorganização das relações econômicas em torno de mercados multilaterais, que foram especialmente pesquisados e teorizados na área de negócios. As relações de mercado tradicionais, em contexto pré-digital, com algumas exceções notáveis, tendem a ser unilaterais, com uma empresa negociando diretamente com os compradores. Por outro lado, as plataformas constituem mercados bilaterais, ou cada vez mais complexos multilaterais, que funcionam como agregadores de transações entre usuários finais e uma grande variedade de terceiros. Um exemplo clássico de um mercado bilateral semelhante à App Store é um console de *games* como o PlayStation, que conecta as empresas de games aos jogadores (*Ibid.*, tradução nossa).

⁵¹ Em terceiro lugar, as plataformas orientam não apenas as transações econômicas, mas também as interações dos usuários. Isso nos leva à dimensão da governança, que foi colocada na agenda de pesquisa especialmente pela economia política e pelos estudos de *software*. Mais visivelmente, as plataformas estruturam como os usuários finais podem interagir entre si e com os complementadores por meio de interfaces gráficas do usuário, oferecendo vantagens específicas enquanto retêm outras, por exemplo, na forma de botões – curtir, seguir, avaliar, comprar, pagar – e de métricas relacionadas a eles. Essa forma de governança das plataformas materializa-se por meio de classificação algorítmica, privilegiando sinais de dados específicos em detrimento de outros, moldando assim os

Em decorrência desse movimento, Nick Srnicek entende que esse estágio da rede é o do “capitalismo de plataforma”, pois as empresas dominantes da *internet* operam nesse modelo de negócio. Assim, para o autor, as plataformas apresentam-se como intermediárias⁵², permitindo que a oferta encontre a demanda. Mas, além disso, as plataformas definem os mercados, desenhando as regras de interação entre seus usuários, bem como as de geração e de distribuição de valor no seu sistema⁵³.

Com a consolidação do capitalismo de plataforma, observam-se os efeitos provocados nas relações de consumo, como, por exemplo, na figura do consumidor. Este, por sua vez, não se enquadra apenas na definição legal proposta pelo artigo 2.º do Código de Defesa do Consumidor (CDC) como destinatário final do bem⁵⁴; na realidade, ele é mercadoria e promotor dos próprios produtos e serviços que consome. Daí o surgimento da figura do *prosumer*⁵⁵.

Logo, além de consumir, o usuário, por meio das avaliações e dos comentários sobre os produtos feitos nos *sites* e de seus *feedbacks* nas redes sociais destinados a outros consumidores, acaba parametrizando o próprio movimento do consumo⁵⁶, atuando como uma figura ativa no mercado. Portanto, o consumidor não apenas adquire como também promove o bem e o serviço de consumo⁵⁷. Além de assumir o papel de promotor dos modelos de negócios dos *players*, o consumidor também figura como mercadoria para as plataformas, em razão da utilização dos seus dados pessoais, mormente explorados para assédio de consumo por meio do *marketing*, como será visto. Assim, o conceito de consumidor como destinatário final está cada vez mais fragilizado com os novos modelos de mercado no ciberespaço.

tipos de conteúdo e serviços que se tornam visíveis e em destaque e o que permanece amplamente fora do alcance (*Ibid.*, tradução nossa).

⁵² SRNICEK, Nick. *Platform Capitalism*. Cambridge: Polity Press, 2017. p. 44.

⁵³ *Ibid.*, p. 47.

⁵⁴ “Art. 2.º Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final” (BRASIL. Lei n.º 8.078, de 11 de setembro de 1990. Institui o Código do Consumidor. *Diário Oficial da União*: seção 1, Brasília, DF, Suplemento, p. 1, 12 set. 1990. PL 3683/1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078.htm. Acesso em: 14 jan. 2022).

⁵⁵ “Web 2.0 technologies were seen as blurring the boundaries between production and consumption, giving rise to new forms of user participation as part of an online ‘participatory culture’” (HELMOND, Anne. *The Platformization of the Web: Making Web Data Platform Ready*. *Social Media + Society*, Sept. 30, 2015).

⁵⁶ “A internet e sua camada de aplicações, principalmente a *web* com *blogs*, redes sociais, *websites* etc., capilarizou esses painéis de opiniões. Os consumidores compartilham e trocam, com mais frequência, em diversos canais e quase em tempo real, informações sobre as suas experiências de consumo: um *blog* em que consumidores de vinho comentam as suas aspirações de *sommelier*, ou simplesmente, um consumidor que reclama sobre uma determinada funcionalidade do produto em uma rede social. Em todas essas situações, eles passam a ser ‘ouvidos’ por seus milhares de pares, parametrizando o próprio movimento de consumo” (BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 12).

⁵⁷ “O consumidor deixa, portanto, de ter uma posição meramente passiva no ciclo do consumo. Ele passa a ter uma participação ativa, que condiciona a própria confecção, distribuição e, em última análise, a segmentação do bem de consumo, transformando-se na figura do *prosumer*. O consumidor não apenas consome (*consumption*), mas, também, produz o bem de consumo (*production*): *prosumer*” (*Ibid.*, p. 13).

Com a hiperconectividade dos usuários-consumidores nas plataformas, os dados pessoais estão em abundância no ciberespaço, revelando informações sobre hábitos de consumo, personalidade e outros conhecimentos importantes para as tomadas de decisões das companhias. Como o novo modelo do capitalismo baseia-se nas informações⁵⁸, iniciou-se uma corrida para coletar o máximo possível de informações dos usuários.

A revolução tecnológica e o *Big Data* ofereceram as ferramentas necessárias para a organização de forma escalável dos dados dos consumidores. Iniciou-se, assim, a formação de um banco de dados por empresas, de dados não só quantitativos, mas, especialmente, qualitativos, com informações preciosas sobre hábitos de consumo, o que gerou uma economia da vigilância⁵⁹. A partir desse momento, a ciência do *marketing* passou por uma profunda transformação, pois, com os bancos de dados comportamentais sobre os consumidores, tornou-se possível abordá-los de forma personalizada.

1.1.2 Publicidade comportamental: o assédio constante

Marketing pode ser definido como “um processo de análise e obtenção de informações sobre os desejos do consumidor”⁶⁰ ou como um “conjunto de atividades e operações que ocorrem desde a criação de um produto (ou serviço) até a sua destruição (término da sua vida útil) pelo consumidor final”⁶¹.

O processo do *marketing* vai desde a concepção do produto até o pós-venda. Trata-se de uma prática de investigação e de análise das necessidades e das práticas do mercado⁶². Uma das técnicas de *marketing* é a publicidade, mas, ressalta-se, não se confundem. A publicidade possui uma função comercial com o objetivo de lucro, o que a torna uma atividade de caráter econômico⁶³. A publicidade é um instrumento do *marketing*, sendo um dos mais importantes

⁵⁸ CASTELLS, Manuel. *Sociedade em rede*. Tradução de Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 1998. v. 1, p. 119.

⁵⁹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 12.

⁶⁰ AFONSO, Luiz Fernando. *Proteção do consumidor: propaganda enganosa e prática do storytelling*. São Paulo. Almedina, 2020, p. 50.

⁶¹ LOPES, Maria Elisabete Vilaça. O consumidor e a publicidade. *Revista de Direito do Consumidor*, São Paulo, n. 1, mar. 1992, p. 149.

⁶² “Isto significa dizer que o *marketing* empresarial acompanha o produto desde o seu nascedouro, antes mesmo do seu nascimento, até a realização da venda e também durante a pós-venda. O *marketing*, antes da concepção, analisa e investiga as necessidades e anseios do mercado. Concebido o produto, o objetivo do *marketing* volta-se para sua colocação (compra-e-venda mercantil ou aquisição do serviço). Realizada a venda, as ações de *marketing* continuam, no sentido de proporcionar ao consumidor a plena fruição do bem ou serviço adquirido, estabelecendo as estratégias de garantia e assistência técnica” (LOPES, *loc. cit.*).

⁶³ AFONSO, *loc. cit.*, p. 49-50.

meios utilizados pelos fornecedores para despertar um desejo de compra dos consumidores⁶⁴, inserindo-se no movimento de despersonalização das relações privadas⁶⁵.

Dessa maneira, a publicidade é “o conjunto de meios destinados a informar o público e a convencê-lo a adquirir um bem ou serviço”⁶⁶. Claudia Lima Marques salienta que a publicidade passa a integrar o contrato firmado com o consumidor, sendo considerada uma cláusula extra não escrita, mas cujo cumprimento poderá ser exigido, mesmo na forma de litígio, no Judiciário⁶⁷. Com o novo paradigma tecnológico, as práticas de *marketing* sofisticaram-se em função das novas ferramentas oferecidas, especialmente com o *Big Data*.

Em seu desenvolvimento, a publicidade passou por algumas fases: contextual, segmentada e comportamental (agora). Na fase contextual, buscava-se aliar o ambiente em que o consumidor está inserido ao objeto de consumo anunciado, por meio analógico ou digital. Dessa maneira, em vez de realizar uma publicidade nos comerciais de televisão, onde não há uma homogeneidade de interesses dos consumidores, busca-se direcionar a mensagem publicitária para um grupo que possua uma predisposição a se interessar pelo bem ou pelo serviço oferecido⁶⁸. Já a publicidade segmentada foca o *aspecto subjetivo*, isto é, no próprio público-alvo do bem ofertado⁶⁹. O que importa não é o ambiente em que será “disparada” a publicidade, mas o público que tem acesso ao conteúdo. Logo, se o bem de consumo é direcionado ao público adolescente, a crianças ou a idosos, para realizar uma abordagem segmentada, a publicidade será realizada em ambientes em que predomine esse público-alvo⁷⁰. Por sua vez, a publicidade comportamental, espécie de publicidade direcionada, é realizada por via digital, permitindo uma personalização nunca alcançada nas fases anteriores em razão do acesso aos dados comportamentais. Como salienta Bioni, os usuários convertem-se em consumidores no ciberespaço⁷¹, o que demonstra a imersão e a razão do crescimento do comércio eletrônico. A publicidade comportamental também é conhecida por termos como

⁶⁴ *Ibid.*, p. 51.

⁶⁵ BIONI, *loc. cit.*, p. 14.

⁶⁶ LOPES, *op. cit.*, p. 150.

⁶⁷ MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p. 849.

⁶⁸ “Por exemplo, há uma maior probabilidade de que leitores de revistas de carros tenham interesses na aquisição de tal bem, já que se subentende que quem está pesquisando sobre o assunto tende a ser um potencial comprador. Do mesmo modo, o anúncio de um livro sobre política tende a ser mais efetivo se hospedado no caderno de política de um determinado jornal, uma vez que os leitores daquele caderno específico têm predileção sobre tal assunto. Direciona-se, assim, a publicidade em um ambiente propício para captar a atenção do consumidor, facilitando-se, pois, o encontro entre comprador e vendedor, que é o desiderato da publicidade” (BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 15).

⁶⁹ BIONI, *loc. cit.*

⁷⁰ BIONI, *loc. cit.*

⁷¹ *Ibid.*, p. 16.

redirecionamento e *microtargeting*. Trata-se de uma abordagem personalizada a partir da coleta de dados comportamentais dos consumidores.

A publicidade, que sempre foi um jogo de adivinhação e de sedução, transformou-se em uma prática que oferece previsibilidade aos anunciantes, isto é, opera com o objetivo de entregar uma mensagem específica a uma pessoa determinada no exato momento em que essa mensagem tem alta probabilidade de influenciar de fato a vontade do indivíduo – Santo Graal da publicidade⁷².

Como a ciência mercadológica percebe a potencialidade da abordagem personalizada comportamental, o comércio digital está repleto de publicidades *on-line* que tentam induzir o usuário-consumidor ao consumo. Por meio de *cookies*⁷³, *fingerprinting*⁷⁴, *flash-cookies* e outras técnicas de rastreamento, as empresas monitoram cotidianamente os usuários para conseguirem acertar seus alvos. Observa-se uma constante evolução das técnicas de *tracking*, como, por exemplo, a mudança dos ordinários *cookies* para os *flash-cookies*.

A criação desses novos *cookies* ocorreu quando programadores aproveitaram um recurso do *Adobe's Flash MX*. Esses *cookies* têm maior capacidade de armazenamento de informações⁷⁵.

⁷² ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 96.

⁷³ “Os *cookies*, assim como os arquivos de log, de acordo com a NRPOL – Norma de Referência da Privacidade On-line – Versão 1.0, de junho de 2000, são considerados meios não-explícitos de coleta de informações on-line, usados pela empresa para interagir, registrar ou monitorar as atitudes de usuários em visita a seu website, para quaisquer finalidades (item 5.10). Os *cookies*, os famosos biscoitinhos da Web, têm dado dor de cabeça aos usuários, preocupados com sua privacidade. São pequenos arquivos de textos que são gravados no computador do usuário, pelo browser, quando ele visita determinados sites do comércio eletrônico. Têm por escopo guardar alguns dados, como nomes e senhas, para que, quando o usuário retorne a determinados sites, não precise digitar tudo novamente. Para as páginas comerciais, outra é a utilidade dos *cookies* que elas distribuem. Utilizam-nos para direcionar os anúncios com base nos interesses e no comportamento do usuário. As informações coletadas pelos *cookies* são chamadas de ‘sequência de cliques’ ou ‘rastreamento de cliques’, que também podem descrever quais páginas o usuário visitou em cada loja do vendedor” (ZANELATO, Marco Antonio. *Condutas ilícitas na sociedade digital*. *Revista de Direito do Consumidor*, São Paulo, n. 44, out./dez. 2002, p. 216-217).

⁷⁴ “Most or all of the information provided by your browser to websites and third parties can be used to fingerprint your device and to track you. As long as a piece of information is at least somewhat stable over time, it can be leveraged in a fingerprint. This can include things as innocuous as the size of your browser window, the version number of your browser, or even the set of fonts installed on your computer. Imagine that an online tracker derives a fingerprint for you that consists of, say, 43 different features. After the tracker first sees you, however, you install two new fonts on your computer. When the tracker sees you again, you’ll have a fingerprint with 45 features, of which 43 will match the previous observation. Much like observations of actual fingerprints, two such observations that differ slightly can still be linked through statistical means. In the industry, these fingerprints are often called ‘statistical IDs’” (NARAYANAN, Arvind; REISMAN, Dillon. *The Princeton Web Transparency and Accountability Project*. In: CERQUITELLI, Tania; QUERCIA, Daniele; PASQUALE, Frank (ed.). *Transparent data mining for Big and Small Data*. [S.l.]: Springer, 2017, p. 9-10. Disponível em: <https://www.cs.princeton.edu/~arvindn/publications/webtap-chapter.pdf>. Acesso em: 15 mar. 2022).

⁷⁵ “‘United Virtualities’ PIE leveraged a feature in Adobe’s Flash MX: the ‘local shared object’, also known as the ‘flash cookie’. Flash cookies offer several advantages that lead to more persistence than standard HTTP cookies. Flash cookies can contain up to 100KB of information by default (HTTP cookies only store 4KB)” (SOLTANI, Ashkan; CANTY, Shannon; MAYO, Quentin; THOMAS, Lauren; HOOFNAGLE, Chris J. *Flash Cookies and Privacy*. In: AAI SPRING SYMPOSIUM SERIES. Palo Alto, California, 2010, p. 158. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862. Acesso em 09 Fev 2023).

Além disso, é mais difícil eliminá-los do que os *cookies* HTTP (do inglês, *Hypertext Transfer Protocol*), pois não há uma data de expiração na sua concepção; instalam-se em um local diferente dos *cookies* ordinários, o que dificulta sua localização e consequente eliminação⁷⁶.

O cenário agrava-se quando se nota que a maioria das plataformas utiliza tecnologias mais intrusivas, como os *flash-cookies*⁷⁷ e as técnicas de *fingerprinting*⁷⁸. Com efeito, o rastreamento dos usuários permite a criação de um retrato dos interesses dos consumidores. Assim “a abordagem publicitária passa a ser atrelada com precisão ao perfil do potencial comprador”⁷⁹. Além de ser mais eficaz na persuasão do consumidor, a abordagem publicitária comportamental também reduz os custos da ação publicitária⁸⁰, pois é uma abordagem meticulosamente orquestrada, sabendo o que oferecer e o momento para tal.

Outros instrumentos também são utilizados para o direcionamento segmentado de conteúdos, produtos e serviços, como o *clickstream*, isto é, a prática de analisar todos os conteúdos clicados durante a navegação dos usuários, para assim despejar quantidades abundantes de ofertas em diversos meios digitais, como *telemarketing* e *spam* nos *e-mails*⁸¹.

Essa prática constante de monitoramento e de disparo de publicidades a partir de dados comportamentais configura-se como assédio de consumo aos consumidores. Para Herman Benjamin, o assédio de consumo é uma estratégia de *marketing* muito agressiva, resultante de

⁷⁶ “Flash cookies do not have expiration dates by default, whereas HTTP cookies expire at the end of a session unless programmed to live longer by the domain setting the cookie. Flash cookies are stored in a different location than HTTP cookies, thus users may not know what files to delete in order to eliminate them” (SOLTANI, Ashkan; CANTY, Shannon; MAYO, Quentin; THOMAS, Lauren; HOOFNAGLE, Chris J., *loc. cit.*).

⁷⁷ “We encountered Flash cookies on 54 of the top 100 sites. These 54 sites set a total of 157 Flash shared objects files yielding a total of 281 individual Flash cookies. Ninety-eight of the top 100 sites set HTTP cookies (only wikipedia and wikimedia.org lacked HTTP cookies in our tests). These 98 sites set a total of 3,602 HTTP cookies. Thirty-one of these sites carried a TRUSTe Privacy Seal. Of these 31, 14 were employing Flash cookies. Thus, both HTTP and Flash cookies are a popular mechanism on top 100 websites” (SOLTANI, Ashkan; CANTY, Shannon; MAYO, Quentin; THOMAS, Lauren; HOOFNAGLE, Chris J. *Flash Cookies and Privacy*. In: AAAI SPRING SYMPOSIUM SERIES. Palo Alto, California, 2010, p. 160).

⁷⁸ “This study was done in 2014, and didn’t use OpenWPM, as it wasn’t mature yet. In 2016, we began WebTAP’s monthly 1-million-site measurements using Open WPM. We’ve found that virtually every HTML5 API *is being abused to fingerprint devices*” (NARAYANAN, Arvind; REISMAN, Dillon. The Princeton Web Transparency and Accountability Project. In: CERQUITELLI, Tania; QUERCIA, Daniele; PASQUALE, Frank (ed.). *Transparent data mining for Big and Small Data*. [S.l.]: Springer, 2017, p. 11, grifo nosso. Disponível em: <https://www.cs.princeton.edu/~arvindn/publications/webtap-chapter.pdf>. Acesso em: 15 mar. 2022).

⁷⁹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 17.

⁸⁰ BIONI, *loc. cit.*

⁸¹ “A partir do acesso ao *profile* tornam-se frequentes as práticas de direcionamento de publicidade *online* abusivas que constituem assédio ao consumidor: o usuário é interpelado por uma grande quantidade de ofertas de produtos através de diversos meios, incluindo práticas de *telemarketing*, mensagens telefônicas e recebimento de *e-mails*; transformando as relações de consumo atuais no que Tim Wu denomina de mercado da *atenção*” (BORGES, Gustavo; FILÓ, Maurício da Cunha S. Consumo, publicidade e inteligência artificial: (necessários) limites à tecnologia persuasiva no constante assédio do consumidor. *Revista de Direito do Consumidor*, São Paulo, v. 30, n. 136, jul./ago. 2021, p. 212).

práticas de *targeting* em grupo de consumidores⁸², que são expostos a cada navegação *on-line* a diversos tipos de produtos e serviços.

Segundo Claudia Lima Marques, o comércio eletrônico consolidou novas práticas abusivas, que em sua visão escapam da disciplina do artigo 39 do CDC, não por não estarem previstas, mas pelo seu grau de sofisticação tecnológica, sendo necessária uma aplicação qualificada da boa-fé.⁸³ Esse assédio de consumo fragiliza a autonomia dos usuários, impedindo decisões racionais⁸⁴. O legislador entendeu que todas as práticas comerciais agressivas que impactam a autonomia dos consumidores representam assédio de consumo⁸⁵.

O assédio de consumo pode até atingir um elevado grau de coação dos consumidores, ocasionando um constrangimento⁸⁶. Cabe destacar, porém, que o assédio, especialmente na *internet*, ocorre por meio de práticas “invisíveis”, indiretas e sutis⁸⁷, como no aparecimento cotidiano de um produto que o consumidor visitou há semanas nos *sites* navegados como forma de atrair o consumo. Em função dessas práticas, o consumidor encontra-se vulnerável comportamentalmente no ciberespaço, isto é, sua autodeterminação fica fragilizada em razão das práticas de *marketing* comportamental, agravando-se a denominada vulnerabilidade comportamental⁸⁸.

⁸² “Nos Projetos de Lei do Senado Federal que visam a atualização do CDC, a Comissão de Juristas, coordenada pelo e. Min. Antônio Herman Benjamin, introduziu no direito brasileiro a figura do combate ao assédio de consumo, nominando estratégias assediosas de marketing muito agressivas e de marketing focado em grupo de consumidores, *targeting*, muitas vezes nos mais vulneráveis do mercado, idosos e adolescentes” (MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p. 931).

⁸³ MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p. 930.

⁸⁴ “O assédio de consumo trabalha o convencimento do consumidor a partir de fatores de influência variados, como a difusão de um risco, ou pela sugestão de envolvimento com o produto ou com a respectiva marca, minando a possibilidade de uma decisão racional plena do consumidor” (VERBICARO, Dennis; RODRIGUES, Lays; ATAÍDE, Camille. Desvendando a vulnerabilidade comportamental do consumidor: uma análise jurídico-psicológica do assédio de consumo. *Revista de Direito do Consumidor*, São Paulo, v. 27, n. 119, set./out. 2018, p. 352).

⁸⁵ “A opção do legislador brasileiro foi de considerar assédio de consumo o gênero para todas as práticas comerciais agressivas que limitam a liberdade de escolha do consumidor” (MARQUES, *op. cit.*, p. 931).

⁸⁶ “O assédio de consumo coloca o consumidor em uma situação em que se vê constrangido, persuadido e pressionado a adquirir os bens considerados desejáveis e ‘necessários’ no momento, que, por sua vez, subitamente tornam-se ultrapassados e são substituídos por outros, num ciclo vicioso de consumo, impossível de ser acompanhado nem mesmo pelo consumidor mais diligente, gerando consequências psicológicas (ansiedade, frustração e, numa escala mais grave, depressão) e econômicas (comprometimento financeiro e superendividamento). É nesse descompasso entre o que se deseja, o que se impõe e o que se pode adquirir que o assédio de consumo se instala e coloca o consumidor em uma situação de vulnerabilidade extremada” (VERBICARO; RODRIGUES; ATAÍDE, *loc. cit.*, p. 356-357).

⁸⁷ “Importante ressaltar que o assédio de consumo não se resume a práticas violentas e manifestamente visíveis. Ao contrário, compreende também condutas tendentes a elidir, ainda que de forma indireta e por vezes até sutil, a razão e a liberdade de escolha dos indivíduos absorvidos pela sociedade de consumo, inebriando suas percepções a partir de uma espetacularização da vida” (*Ibid.*, p. 357).

⁸⁸: “Para tanto, a análise dos aspectos psicológicos deve ser feita sob a ótica da existência de uma aproximação com a ideia da vulnerabilidade comportamental do consumidor, sobretudo se considerarmos que o assédio de

Verifica-se, portanto, que os dados comportamentais dos usuários permitiram uma grande transformação do *marketing*, assim como aumentaram os riscos para os consumidores. O monitoramento constante dos consumidores gera uma perda de controle dos usuários sobre seus dados e um agravamento das suas vulnerabilidades, o que influi diretamente no fluxo informacional dos dados pessoais. Com efeito, o ciberespaço tornou-se uma espécie de Panóptico, como imaginado por Jeremy Bentham, por ser uma arquitetura que permite vigiar sem ser visto, tornando tudo visível enquanto o observador permanece invisível⁸⁹.

Se antes a figura centralizada do Estado no *Big Brother* constituía um dos grandes medos da modernidade, o panóptico digital permitiu a criação de diversos *Big Other*⁹⁰, que estão rastreando os consumidores, em especial, por meio dos *smartphones*, que possibilitam uma vigilância fluida e constante, seja *on-line*, seja *off-line*. De fato, as plataformas sabem onde os usuários estão graças à localização geográfica do *global positioning system* (GPS)⁹¹ instalados nos dispositivos.

Portanto, o *marketing*, sem dúvida, impactou diretamente os direitos dos consumidores, como se percebe no incitamento das vulnerabilidades e na depredação da proteção de dados dos consumidores no ciberespaço. Desse modo, torna-se fundamental indagar: por que o *marketing* é tão importante para as plataformas no contexto do capitalismo de vigilância?

A resposta é financeira. A publicidade representa a maior fonte de faturamento das plataformas, como se observa no *Facebook*, cuja receita em publicidade representa 98% do seu faturamento, correspondendo ao valor de 86 bilhões de dólares⁹². A *Alphabet – holding* que controla o *Google* e o *Youtube* –, por exemplo, revelou em seus resultados do quarto trimestre de 2021 que a publicidade faturou US\$ 61,24 bilhões no trimestre. Nesse montante, está o valor

consumo visa influenciar justamente no comportamento dos indivíduos, incutindo desejos e necessidades de forma invasiva e tenaz” (VERBICARO; RODRIGUES; ATAÍDE, *loc. cit.*).

⁸⁹ RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 47.

⁹⁰ “These developments became the basis for a fully institutionalized new logic of accumulation that I have called surveillance capitalism. In this new regime, a global architecture of computer mediation turns the electronic text of the bounded organization into an intelligent world-spanning organism that I call Big Other” (ZUBOFF, Shoshana. *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*. *Journal of Information Technology*, [s.l.], 2015, p. 85. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754. Acesso em: 19 mar. 2022.

⁹¹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 19.

⁹² FRANEK, Kamil. *How Facebook Makes Money: Business Model Explained*. *Kamil Franek*, April 2021. Disponível em: <https://www.kamilfrank.com/how-facebook-makes-money-business-model-explained/>. Acesso em: 19 mar. 2022.

arrecadado pelo *Youtube*, que alcançou a marca de US\$ 8,63 bilhões⁹³, sendo a principal receita dessa plataforma, conforme aponta seu próprio *site* institucional⁹⁴. Mesmo sendo uma varejista, os ganhos em publicidade comportamental da *Amazon* representam um terceiro pilar do faturamento da empresa, correspondendo a um mercado de 125 bilhões de dólares⁹⁵, que ajuda a empresa a expandir-se em grande escala.

Dessa forma, por meio dos instrumentos tecnológicos, as abordagens comerciais tornaram-se cada vez mais personalizadas em razão da lucratividade dessa atividade. Essa personalização é compatível com a nova sociedade dos indivíduos, que demanda um consumo individualizado, almejando serviços a partir dessa demanda: “o que eu quero, quando, onde e como quero”⁹⁶, como se observa nos serviços “*On demand*”.

Nessa lógica da personalização, impulsionada pelos novos desejos do consumidor, o vulnerável fica translúcido, resultando, para Susanne Lace, na figura do “consumidor de vidro”. Para a autora, “as propriedades e capacidades do vidro – fragilidade, transparência e capacidade de distorcer o olhar do observador – [espelham] nossa própria potencial vulnerabilidade⁹⁷”.

Ao fornecer grandes quantidades de dados, a publicidade obteve a capacidade de conhecer os consumidores de vidro com detalhes. Desse modo, todos os usuários são classificados, categorizados e pontuados em centenas de modelos com base em suas preferências. Essa personalização, de certo modo, até auxilia na busca por serviços e produtos, mas, em uma análise mais profunda e crítica, esse modelo gera assédio de consumo e submete os usuários a publicidades predatórias, que exploram suas vulnerabilidades para obter seus lucros, como bem explicita O’Neil nos casos de certas universidades dos Estados Unidos⁹⁸.

⁹³ LOPES, Marco Antônio. Alphabet, dona do Google (GOGL34): lucro sobre e receita supera consenso; ações disparam. *Suno notícias*, 1.º fev. 2022. Disponível em: <https://www.suno.com.br/noticias/alphabet-google-lucro-sobre-receita-4t21/>. Acesso em: 31 mar. 2022.

⁹⁴ “YouTube’s main source of revenue is advertising. Additionally, we earn money from our monthly subscription businesses such as YouTube Premium. We’ve also developed tools to help eligible creators earn money in a variety of other ways, such as Super Chat, channel memberships and merchandise. In most cases, creators and YouTube share revenue generated from these channels” (HOW does YouTube make money? *Youtube*, [20--]. Disponível em: <https://www.youtube.com/howyoutubeworks/our-commitments/sharing-revenue/>. Acesso em: 19 mar. 2022.

⁹⁵ WEISEC, Karen. A Amazon sabe quem você é e do que gosta. E ganha bilhões de dólares com isso. *Gazeta do Povo*, 9 fev. 2019. Disponível em: [https://www.gazetadopovo.com.br/economia/a-amazon-sabe-quem-voce-e-e-do-que-voce-gosta-e-ganha-bilhoes-de-dolares-com-isso-bchtf7mvg2dr7nvxtmxkk45gb/#:~:text=O%20neg%C3%B3cio%20de%20publicidade%20da%20Amazon%20vale%20cerca,aparecer%20perto%20de%20resultados%20de%20busca%20de%20produtos](https://www.gazetadopovo.com.br/economia/a-amazon-sabe-quem-voce-e-e-do-que-voce-gosta-e-ganha-bilhoes-de-dolares-com-isso-bchtf7mvg2dr7nvxtmxkk45gb/#:~:text=O%20neg%C3%B3cio%20de%20publicidade%20da%20Amazon%20vale%20cerca,aparecer%20perto%20de%20resultados%20de%20busca%20de%20produtos.). Acesso em: 19 mar. 2022.

⁹⁶ ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 44-45.

⁹⁷ “Earlier, this was visualized as the life of the glass consumer. The properties and capacities of glass – fragility, transparency, the ability to distort the gaze of the viewer – mirrored our own potential vulnerability” (LACE, Susanne (ed.). *The Glass Consumer: Life in a surveillance society*. Bristol: Policy Press, 2005, p. 7, tradução nossa).

⁹⁸ O’NEIL, Cathy. *Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a*

Zuboff sustenta que o rastreamento dos padrões de comportamento dos usuários no ambiente digital criou um mercado denominado “mercado futuro comportamental”. Nesse mercado, as empresas apostam no comportamento futuro dos usuários, antecipando suas predileções para vender produtos e serviços a partir de análises das personalidades, das emoções e até das vozes dos usuários⁹⁹. Por exemplo, o *Facebook* é capaz de descobrir, por meio de algoritmos, quando um usuário se apaixona e começará um relacionamento podendo, com base nessa informação, iniciar um *marketing* comportamental, direcionando anúncios de viagens românticas, lojas de chocolates e outros bens de consumo que interessam a um casal¹⁰⁰.

Todo esse cenário fez emergir, para Shoshana Zuboff, um capitalismo de vigilância. Ressalta-se, porém, que o capitalismo da vigilância não se restringe à coleta e ao tratamento de dados pela publicidade *on-line* e pelas relações de consumo; a sua dimensão transcende essas ações, pois diz respeito à transformação do capitalismo em um modelo que utiliza a experiência humana como sua matéria-prima.

1.2 A ERA DO CAPITALISMO DE VIGILÂNCIA: SEUS IMPACTOS NOS CONSUMIDORES

Zuboff, em sua densa e importante obra *A era do capitalismo de vigilância*, destaca que o capitalismo de vigilância “reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais”¹⁰¹. Esses dados, por sua vez, alimentam complexos e inacessíveis processos de fabricação conhecidos como inteligência de máquina, que consegue produzir produtos de predição, servindo para antecipar o que o consumidor faria mais cedo ou mais tarde. Uma parte dos dados é “reinvestida” no aprimoramento de produtos e serviços, contudo, o restante é, para a autora, *superávit comportamental*. Esse superávit permitiu a criação do denominado mercado futuro comportamental, um tipo de mercado cujo objetivo é prever os interesses e predileções dos

democracia. Tradução de Rafael Abraham. Santo André, SP: Editora Rua de Sabão, 2020, p. 109 *et seq.*

⁹⁹ “Por fim, esses produtos de predição são comercializados num novo tipo de mercado para predições comportamentais que chamo de *mercados de comportamentos futuros*. Os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro” (ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 19).

¹⁰⁰ MORRIS, Ian. Facebook Knows When You Fall in Love, And That's Pretty Creepy. *Forbes*, Dec. 31, 2016. Disponível em: <https://www.forbes.com/sites/ianmorris/2016/12/31/facebook-knows-when-you-fall-in-love-and-thats-pretty-creepy/#51fef6c16f52>. Acesso em: 29 jun. 2021.

¹⁰¹ ZUBOFF, *loc. cit.*, p. 18.

consumidores. Dessa maneira, os dados servem para antecipar os gostos dos usuários, mas, principalmente, atuam como meio de modificação de comportamento¹⁰².

A professora de Harvard define esse capitalismo como uma nova ordem econômica que reivindica a experiência humana como matéria-prima gratuita para práticas comerciais dissimuladas de extração, previsão e vendas. Além disso, a produção de bens e serviços é subordinada a uma nova arquitetura global de modulação de comportamento.

Aproveitar-se das experiências humanas como matéria-prima foi possível graças a uma institucionalização do sigilo e ao beneficiamento do neoliberalismo, que se espalhou pelos Estados e pela sociedade. Ressalte-se que não se pretende aqui aprofundar o neoliberalismo e suas correntes, seja porque o tema foge do escopo do trabalho, seja porque ele demanda um saber especializado; o objetivo é apenas demonstrar sua importância para a consolidação do capitalismo de vigilância como modelo de negócio na *internet*.

Zuboff sustenta que a ideologia de Hayek forneceu racionalidade às corporações capitalistas de vigilância, surgindo, assim, a aversão à regulação, à supervisão estatal e social e uma simpatia profunda pela autorregulação¹⁰³. Segundo a lógica neoliberal, toda regulação é opressiva, e a burocracia é uma forma de dominação humana que deve ser repudiada¹⁰⁴. Para Pasquale, criou-se uma ideologia ciberlibertária¹⁰⁵. Para manter a glorificada autorregulação, há uma inapropriada relação entre Estado e grandes corporações tecnológicas, que, assim como outros setores, buscam evitar ao máximo demandas regulatórias e de *accountability*. Como bem explica Wendy Brown, a arte de governo neoliberal corrói as redes protetoras sociais de um Estado administrativo, visando destruir os ideais de sociedade, solidariedade e justiça social de maneira normativa, conceitual e prática para conceber um novo *modus operandi*, que atua de baixo para cima¹⁰⁶. Filiando-se aos ensinamentos de Foucault, Brown entende o neoliberalismo como uma forma de pensar, um estilo de vida, uma racionalidade.

¹⁰² *Ibid.*, p. 18-19.

¹⁰³ “A ideologia de Hayek forneceu, do ponto de vista intelectual, a superestrutura e legitimação para uma nova teoria da empresa que se tornou outro antecedente fundamental para a corporação capitalista de vigilância: sua estrutura, conteúdo moral e relação com a sociedade” (ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 53).

¹⁰⁴ “Conforme prediz a influência de Hayek e Friedman, o tema dominante nessa literatura era a ‘natureza coercitiva de governo administrativo’ e a sistemática confluência de regulação da indústria com ‘tirania’ e ‘autoritarismo’. Segundo essa visão de mundo, toda regulação é opressiva, e a burocracia deve ser repudiada como uma forma de dominação humana” (*Ibid.*, p. 130).

¹⁰⁵ PASQUALE, Frank. *The Automated Public Sphere*. University of Maryland, Francis King Carey School of Law Legal Studies, Research Paper No. 2017-31. Nov. 10, 2017, p. 10. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067552. Acesso em: 2 abr. 2022.

¹⁰⁶ “O ataque neoliberal ao social [...] é fundamental para gerar uma cultura antidemocrática desde baixo, ao mesmo tempo em que constrói e legitima formas antidemocráticas de poder estatal desde cima. A sinergia entre os dois é profunda: uma cidadania cada vez mais não democrática e antidemocrática está mais e mais disposta a autorizar

Com a penetração da racionalidade neoliberal em todos os domínios da vida humana, o Estado mostra-se cada vez mais fragilizado e com dificuldades de exercer sua soberania nacional, enquanto as grandes empresas tecnológicas determinam as pautas econômicas e legislativas. Dessa forma, os países demonstram-se insuficientes para limitar as aspirações dos capitalistas da vigilância, o que agrava as vulnerabilidades dos cidadãos em uma competição global, que precariza as relações humanas¹⁰⁷.

É necessário esclarecer que o capitalismo de vigilância não é uma tecnologia; é uma *lógica* que utiliza a evolução tecnológica, e o mundo digital é fundamental para esse modelo econômico. Também importa deixar claro que o capitalismo de vigilância não é inevitável. Na realidade, surgiu da necessidade de monetização das empresas da *internet*, sendo calculado de forma meticulosa, logo, não se trata de um acidente tecnológico¹⁰⁸. É um sistema arquitetado cuidadosamente, possuindo, inclusive, a característica de autopoiese¹⁰⁹, pois é autorreferente¹¹⁰.

Para Zuboff, *Google* foi o pioneiro do capitalismo de vigilância que se vive na atualidade. Com a criação da empresa, na década de 90 do século XX, como um buscador, engenheiros da empresa perceberam que os usuários, ao utilizar o serviço, deixavam registrado muito da sua personalidade. Assim, notou-se que os fluxos contínuos de dados comportamentais colaterais poderiam ser uma excelente munição para aperfeiçoar o algoritmo de busca por meio de sistemas de aprendizagem de máquina. Desse modo, todas as ações dos usuários tornaram-se objeto de análise para os funcionários da gigante tecnológica.

um Estado crescentemente antidemocrático. À medida que o ataque ao social derrota a compreensão democrática de sociedade zelada por um povo caracterizado pela diversidade e habilitado a governar a si de forma igualitária e compartilhada, a política se torna um campo de posicionamento extremo e intransigente, e a liberdade se torna um direito de apropriação, ruptura e até mesmo destruição social – seu inimigo declarado” (BROWN, Wendy. *Nas ruínas do neoliberalismo: a ascensão da política antidemocrática no ocidente*. Tradução de Mario A. Marino, Eduardo Altheman C. Santos. São Paulo: Filosófica Politeia, 2019, p. 39).

¹⁰⁷ BROWN, Wendy. *Nas ruínas do neoliberalismo: a ascensão da política antidemocrática no ocidente*. Tradução de Mario A. Marino, Eduardo Altheman C. Santos. São Paulo: Filosófica Politeia, 2019, p. 102.

¹⁰⁸ “Um fato fundamental para a nossa conversa é que o capitalismo de vigilância foi inventado por um grupo específico de seres humanos num tempo e lugar específicos. Não é um resultado inerente à tecnologia digital, tampouco uma expressão necessária do capitalismo de informação. Ele foi elaborado de maneira intencional num momento da história, mais ou menos da mesma forma que os engenheiros e funileiros da Ford Motor Company inventaram a produção em massa na Detroit de 1913” (*Ibid.*, p. 105).

¹⁰⁹ “Maturana e Varela, ao descreverem como se deu a cunhagem do termo autopoiesis, explicam que desejam descrever a autonomia de um organismo vivo ao percebê-lo como um sistema que se autoproduz” (RODRIGUES, Léo Peixoto; NEVES, Fabrício Monteiro. *A sociologia de Niklas Luhmann*. Petrópolis, RJ: Vozes, 2017, p.44).

¹¹⁰ “A conexão digital é agora um meio para fins comerciais de terceiros. Em sua essência, o capitalismo de vigilância é *parasítico e autorreferente*. Ele revive a velha imagem que Karl Marx desenhou do capitalismo como um vampiro que se alimenta do trabalho, mas agora com uma reviravolta. Em vez do trabalho, o capitalismo de vigilância se alimenta de todo aspecto de toda a experiência humana” (ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 20, grifo nosso).

Nesse momento, ainda havia uma simetria na relação entre o usuário e a plataforma, pois o usuário precisava do serviço, da mesma maneira que a companhia precisava dos seus dados comportamentais para aprimorar o serviço. Logo, as pessoas eram o fim do processo¹¹¹.

Entretanto, em meio à crise econômica provocada pela bolha das empresas.com, havia um grande temor de que a empresa seguisse o mesmo rumo de outras *startups* de tecnologia do Vale do Silício, que faliram por não conseguirem transformar seus negócios em modelos lucrativos¹¹². Inicialmente *Google* concentrou-se na venda de suas licenças, o que não se mostrou rentável¹¹³. Em razão das pressões dos investidores, a empresa cedeu a uma das suas convicções¹¹⁴: explorar o mercado de publicidades. É nesse momento que se dá a descoberta do superávit comportamental, revolucionando o capitalismo e impactando os direitos dos consumidores de maneira sem precedentes.

Com efeito, o *Google* passou a usar seus bancos de dados comportamentais e sua *expertise* computacional de aprendizado de máquina para combinar os usuários com publicidades, buscando abordagens que fossem relevantes para os consumidores. Em decorrência dessa nova forma de monetização do serviço oferecido pela plataforma, há uma grande mudança na relação com o usuário: ele não seria mais o fim do serviço, mas a matéria-prima dos capitalistas de vigilância.

Antes de focar esse modelo de negócio, os dados comportamentais eram usados exclusivamente para melhorar os mecanismos de busca, aprimorando o serviço para os seus consumidores. Com o superávit comportamental por meio dos dados, o *Google* utiliza esse excedente comportamental para redirecionar anúncios aos usuários dos serviços. Dessa maneira, as empresas anunciantes tornaram-se os novos consumidores do *Google*, enquanto os usuários são a matéria-prima¹¹⁵.

¹¹¹ *Ibid.*, p. 85-88.

¹¹² “*Start-ups* que, apenas alguns meses antes, haviam recebido avaliações superdimensionadas foram obrigadas a fechar as portas de supetão. Artigos conhecidos, como o ‘Doom Stalks the Dotcoms’, registravam que os preços das ações das ‘firmas de ponta’ da internet, as mais badaladas do Wall Street, estavam ‘de joelhos, quase nocauteadas’, com muitas delas sendo negociadas abaixo do valor de oferta inicial [...]” (ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 90-91).

¹¹³ “As primeiras receitas do *Google* dependiam de acordos de licenciamento exclusivos para prover serviços de internet a portais como o Yahoo! e o BIGLOBE, do Japão. Uma receita modesta também era gerada a partir de anúncios patrocinados ligados a palavras-chaves nas buscas” (*Ibid.*, p. 89).

¹¹⁴ “O *Google* já havia considerado anúncios de publicidade algo de segunda categoria: sua equipe da AdWords era constituída por sete pessoas, sendo que a maioria delas compartilhava com os fundadores uma antipatia geral por anúncios. O tom fora dado na concepção de mecanismo de busca segundo Sergey Brin e Larry Page, presente no notável artigo ‘The Anatomy of a Large-Scale Hypertextual Web Search Engine’, apresentado na Conferência World Wide Web de 1998: “Imaginamos que os mecanismos de busca financiados por publicidade sejam inerentemente parciais aos anunciantes e distantes das necessidades dos consumidores” (ZUBOFF, *loc. cit.*).

¹¹⁵ “Dados comportamentais cujo valor outrora tinha sido ‘aproveitados’ para melhorar a qualidade da busca para os usuários tornam-se agora a matéria-prima central – e exclusiva do *Google* – para a construção de um dinâmico

A invenção da companhia, por meio do aprendizado de máquina, se desenvolveu, pois hoje possui a capacidade de deduzir pensamentos, sentimentos, intenções e interesses de pessoas¹¹⁶. Sendo assim, os usuários deixaram de ser a finalidade da plataforma para se tornarem os meios para fins de outros¹¹⁷.

Zuboff identifica e explica a lógica por trás do capitalismo de vigilância, seus meios de produção, seus produtos e sua localização do mercado. A lógica consiste em transformar as experiências humanas em superávit comportamental para que seus reais clientes, *os anunciantes*, possam realizar publicidades com um grau de previsibilidade nunca oferecido. Essa lógica criou o mercado futuro comportamental, onde são negociados *ativos de vigilância* a partir de um Panóptico digital. O meio de produção do capitalismo de vigilância é a inteligência artificial, pois quem realiza a manufatura dos *ativos de vigilância* são as máquinas complexas e inescrutáveis da companhia, que se alimentam do superávit comportamental para que suas predições sejam mais confiáveis. Logo, os produtos desse modelo capitalista são os produtos de predição, isto é, as probabilidades dos comportamentos no ciberespaço. Tais produtos são negociados nos mercados futuros comportamentais, um novo mercado disruptivo¹¹⁸.

Constata-se, por conseguinte, que os consumidores do *Google* são os fornecedores que fecham parcerias para anúncios. Logo, os usuários não são o produto, como bem destaca Zuboff¹¹⁹. Também é importante desconstruir outro mito sobre esse mercado: os capitalistas de vigilância, como o *Google* e o *Facebook*, não vendem seus bancos de dados. Essas plataformas utilizam esses dados comportamentais como seu *diferencial competitivo* para vender seu

mercado de publicidade on-line. A companhia passaria a obter mais dados comportamentais que o necessário para servir aos usuários. Esse superávit, um superávit comportamental, era o ativo de custo zero capaz de mudar o jogo, desviado da melhora de serviço para uma operação de mercado genuína e altamente lucrativa” (*Ibid.*, p. 100).

¹¹⁶ ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 100.

¹¹⁷ “[...] as invenções do Google destruíram as reciprocidades de seu contrato social original com os usuários. O papel do ciclo de reinvestimento do valor comportamental que um dia alinhara o Google aos usuários mudou de maneira drástica. Em vez de aprofundar a unidade de oferta e demanda com suas populações, o Google optou por reinventar seu negócio em torno da florescente demanda dos anunciantes, ávidos por aproveitar o máximo até raspar o tacho do comportamento on-line por qualquer meio disponível na competição por vantagem no mercado. Na nova operação, os *usuários não eram mais fins em si mesmos, mas tornaram-se meios para fins de outros*” (*Ibid.*, p. 108, grifo da autora).

¹¹⁸ *Ibid.*, p. 114-117.

¹¹⁹ “Não somos mais os *sujeitos* da realização de valor. Tampouco somos conforme alguns insistem, o ‘produto’ das vendas do Google. Em vez disso, somos os *objetos* dos quais as matérias-primas são extraídas e expropriadas para as fábricas de predição do Google. Predições sobre o nosso comportamento são os produtos do Google, e são vendidos aos verdadeiros clientes da empresa, mas não a nós. *Nós somos os meios para fins de outros*” (*Ibid.*, p. 115, grifo da autora).

serviço de publicidades *on-line* às empresas anunciantes, garantindo que, graças aos bancos de dados e à inteligência artificial avançada, a abordagem seja eficaz¹²⁰.

O capitalismo de vigilância fez com que os serviços da *internet*, que um dia foram criados para os usuários, passassem a ser aprimorados tendo em vista seus reais clientes. Dessa maneira, o usuário não é consumidor; os consumidores são as empresas que anunciam seus produtos e serviços. O usuário, na realidade, é apenas a matéria-prima que a plataforma utiliza para angariar novos anunciantes por meio da mensagem de que suas tecnologias promovem a eficiência nas abordagens e até a modulação comportamental. Portanto, o *Google* vende segurança e previsibilidade nas abordagens publicitárias.

A questão é que a extração dos dados comportamentais é unilateral, sem respeito ao consentimento dos usuários. Apropriam-se da vida dos indivíduos sem pedir permissão. Para Van Dijck, esse movimento é fruto do dataísmo, que se caracteriza por objetificar e quantificar todos os tipos de rastreamento de comportamento humano e social por meio das atividades no ciberespaço¹²¹. Além disso, a confiança é outro fator importante: nota-se que os usuários têm *fides* nas plataformas nas práticas de coleta e de tratamento de dados¹²², uma questão importante, que será analisada no próximo capítulo.

O dataísmo é uma crença cega na tecnologia, pressupondo que toda coleta e toda análise de dados são neutras e benéficas, servindo como mola de ampliação de conhecimento para a sociedade, gerando apenas benefícios para a comunidade¹²³. A dataficação é a prática de transformar as experiências e personalidades dos consumidores em dados comportamentais por meio de tecnologias de ponta, inovadoras e sem precedentes. Cria-se, assim, o superávit comportamental a ser explorado e analisado.

¹²⁰ “Os executivos do Google gostam de alegar sua pureza em termos de privacidade porque não vendem a matéria-prima em si. Em vez disso, a empresa vende as previsões que só ela está habilitada para fabricar a partir de sua reserva privada, um volume mundial histórico de superávit comportamental” (*Ibid.*, p. 117).

¹²¹ VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, [s.l.], v. 12, n. 2, 2014, p. 201. Disponível em: https://www.academia.edu/26648535/Datafication_dataism_and_dataveillance_Big_Data_between_scientific_paradigm_and_ideology. Acesso em 09 Fev 2023.

¹²² “[...] in many respects datafication is rooted in problematic ontological and epistemological claims. However, compelling some examples of applied Big Data research, the ideology of *dataism* shows characteristics of a widespread *belief* in the objective quantification and potential tracking of all kinds of human behavior and sociality through online media technologies. Besides, dataism also involves *trust* in the (institutional) agents that collect, interpret, and share (meta)data culled from social media, internet platforms, and other communication technologies” (*Ibid.*, p. 198, grifo do autor).

¹²³ SOUZA, Joyce. Inteligência artificial, algoritmos preditivos e o avanço do colonialismo de dados na saúde pública brasileira. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021, p. 114.

Sabe-se que toda inovação, por ser inédita, traz consigo o desconhecido, expondo os consumidores a riscos. A dataficação tem estreita relação com a utilização da inteligência artificial, pois o aprimoramento do aprendizado das máquinas depende dos dados. Desse modo, o capitalismo de vigilância requer experiências humanas para personalizar seus produtos e serviços.

Para compreender os atores e problemas envolvidos, é importante apresentar os conceitos de inteligência artificial e analisar seus meandros.

1.2.1 Inteligência artificial, *machine learning* e redes convolucionais

A inteligência artificial sempre esteve no imaginário da sociedade ligada à possibilidade de máquinas dominarem os humanos, superando-os em um futuro tecnológico. Essa visão cinematográfica dificulta a compreensão do que é a inteligência artificial e como é utilizada para fins comerciais atualmente. Não há dúvida de que as pesquisas de IA foram impulsionadas pela busca, por meio de métodos computacionais, de alcançar a inteligência humana, mas hoje sua utilização destina-se a diversos tipos de tarefas. A IA revela-se importante e eficiente para realizar uma atividade que até então era privativa dos humanos: detectar problemas-padrão e solucioná-los.

Diferentemente do imaginário apocalíptico coletivo, a inteligência artificial acompanha os indivíduos todos os dias, traçando as rotas do GPS, selecionando os conteúdos nos serviços de *streaming*, direcionando as publicidades nas redes sociais e pela *web*. Além disso, a inteligência artificial, como mostra Cathy O’Neil, é utilizada para avaliar professores, averiguar a probabilidade de reincidência na justiça criminal, classificar os consumidores como dignos ou não de melhores condições de créditos e seguros¹²⁴, assim como é indispensável para a governança das plataformas.

Com efeito, a IA é de suma importância para as empresas que promovem o capitalismo de vigilância, pois, além de automatizar processos repetitivos em grande velocidade, essa tecnologia realiza funções mais complexas, como a administração da plataforma e de suas operações. As plataformas são administradas por IA desde a triagem, indo do desligamento de funcionários até o direcionamento da publicidade aos usuários¹²⁵.

¹²⁴ O’NEIL, Cathy. *Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia*. Tradução de Rafael Abraham. Santo André, SP: Editora Rua de Sabão, 2020.

¹²⁵ ILO. *World Employment and Social Outlook: The role of digital labour platforms in transforming the world of work*. Geneva: ILO, 2021, p. 58. Disponível em:

Os códigos são a base da IA sendo programados para identificar padrões; a partir dessa detecção, é tomada uma decisão. Em síntese, os algoritmos são o alicerce da IA executando determinações a partir de *machine learning* ou *deep learning*. Assim, a IA transforma dados em padrões de informação e logo em conhecimento – como Castells ensina –, o que lhe permite automatizar tarefas, realizar predileções e previsões¹²⁶.

Existem os algoritmos determinísticos – que apresentam comportamento e resultado previsíveis ou, em outras palavras, sempre produzirão a mesma saída (resposta) – e os preditivos – que se utilizam de dados pretéritos para realizar análises estatísticas e prever o futuro, de maneira probabilística¹²⁷. Esses tipos de IA são possíveis por meio do *machine learning* e *deep learning*.

O *machine learning* e o *deep learning* são tipos de IA. O *deep learning* é uma abordagem (*approach*) que usa a técnica de aprendizado de máquina (em inglês, *machine learning*)¹²⁸. O *machine learning* é um aprendizado supervisionado e consiste em alimentar a inteligência artificial com quantidades abundantes de dados para que o código detecte padrões e saiba como resolvê-los. Dessa maneira, deve-se criar um mecanismo de entrada de dados (*input*) para que a máquina consiga identificar *standards* nos dados coletados dos usuários submetidos ao capitalismo de vigilância. Do mesmo modo, é necessário prever o mecanismo de saída (*output*), que é a resposta automatizada do algoritmo após detectar determinada situação¹²⁹.

David Sumpter, ao analisar pesquisas sobre a IA em *videogames* ou jogos de tabuleiros, explica que esse tipo de aprendizado de máquina é uma solução de “cima para baixo”: um programador, de posse de robustos dados, insere no *input* tais informações para que a máquina aprenda, logo, não há um aprendizado próprio da IA¹³⁰.

https://www.ilo.org/wcmsp5/groups/public/@dgreports/@dcomm/@publ/documents/publication/wcms_71749.pdf. Acesso em: 28 jun. 2021.

¹²⁶ CORVALÁN, Juan Gustavo. Inteligencia Artificial GPT-3, PretorIA y Oráculos Algorítmicos en el Derecho. *International Journal of Digital Law*, Belo Horizonte, ano 1, n. 1, jan./abr. 2020, p. 13.

¹²⁷ SOUZA, Joyce. Inteligência artificial, algoritmos preditivos e o avanço do colonialismo de dados na saúde pública brasileira. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021, p. 108-109.

¹²⁸ IBM Developer. What is the Difference Between Deep Learning and Machine Learning? *Youtube*, 30 abr. 2020. 1 vídeo (1:32). Disponível em: <https://www.youtube.com/watch?v=terWb6ja-HM>. Acesso em: 26 mar. 2022.

¹²⁹ NUNES, Dierle; MARQUES, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. *Revista de Processo*, São Paulo, v. 43, n. 285, nov. 2018, p. 423.

¹³⁰ “Por mais impressionantes que sejam, conquistas em jogos de tabuleiro e de cartas exigem que os programadores digam aos algoritmos como resolver o problema usando uma solução de cima para baixo. Eles não se qualificam como contribuições no sentido de encontrar uma forma de inteligência artificial mais geral do tipo de baixo para cima” (SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 232).

Por outro lado, o chamado *deep learning* caracteriza-se por ser um aprendizado não supervisionado por meio de Redes Neurais Artificiais. O matemático inglês explica que o termo “rede neural” descreve um sistema de algoritmos que são inspirados no modo como o cérebro trabalha. Como o cérebro humano é feito de bilhões de neurônios interconectados, que constroem nossos pensamentos por meio de sinais elétricos, as redes artificiais são representações desse processo biológico, gerando uma rede de neurônios virtuais interconectados para produzir uma saída, o resultado¹³¹. Essa abordagem permite um aprendizado de “baixo para cima”, ou seja, a máquina recebe estímulos dos dados¹³², mas encontra a solução sozinha, pois não está totalmente programada.

Tal abordagem revela-se muito mais apropriada para o reconhecimento de padrões e é também mais eficiente, pois não requer uma grande intervenção humana, trabalhando com informações não estruturadas¹³³. São as redes neurais convolucionais¹³⁴ que conseguem, por exemplo, reconhecer automaticamente os rostos dos amigos nas redes sociais¹³⁵, identificar unicamente a face do dono de um *smartphone* para liberar o dispositivo. Solucionam ainda outros problemas que auxiliam as empresas a atingirem seus objetivos comerciais ao fornecerem novas tecnologias para os consumidores¹³⁶.

Como se constata, o capitalismo de vigilância é vital para o aprimoramento dos algoritmos, pois, sem os dados pessoais – única fonte de alimentação dos códigos –, não é

¹³¹ SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 218.

¹³²: “En la IA, las RNA siguen una lógica de estimulación y activación. Reciben estimulación y, según la misma, ‘se activan’ o no. Por eso, la neurona artificial es un conjunto de cálculos o algoritmos que recibe distintos datos de entrada, los evalúa (aprendizaje automático), con datos históricos y lecciones aprendidas y, según el caso, se dispara o no. Así como una neurona biológica puede recibir información simultánea de distintas células, una neurona artificial recibe distintos datos como ‘input’ de la capa de neuronas previa” (CORVALÁN, Juan Gustavo. Inteligencia Artificial GPT-3, PretorIA y Oráculos Algorítmicos en el Derecho. *International Journal of Digital Law*, Belo Horizonte, ano 1, n. 1, jan./abr. 2020, p. 19).

¹³³ “Los sistemas de IA que utilizan RNA, frecuentemente obtienen mejores resultados para reconocer patrones cuando se trata de analizar cantidades masivas de datos (*Big Data*). Son más eficientes, requieren intervención humana reducida y pueden trabajar información que los informáticos llaman ‘no estructurada’ o no organizada bajo criterios concretos. Un Excel con atributos y datos etiquetados es información estructurada. Lo que la gente publica en las redes sociales es un ejemplo de información no estructurada. Las redes neuronales complejas que tienen ‘apas ocultas’, imitan o copian ciertos rasgos de los procesos neuronales de los cerebros humanos, que procesan la información a partir de neuronas, sinapsis, dendritas y axones” (CORVALÁN, *loc. cit.*).

¹³⁴ “Redes neurais convolucionais são uma técnica poderosa porque encontra o tamanho e a forma de padrões importantes automaticamente, sem que os programadores tenham que dizer o que procuram. A ideia de redes neurais convolutas existe desde os anos 1990, mas por um longo tempo elas foram apenas uma, dentre várias diferentes, competindo com algoritmos que foram propostos para ajudar computadores a detectarem padrões” (SUMPTER, *op. cit.*, p. 237).

¹³⁵ *Ibid.*, p. 238.

¹³⁶ “O reconhecimento de faces do Iphone X da Apple utiliza as redes neurais para identificar unicamente o rosto de seu dono. A Tesla utiliza as redes neurais no sistema de visão de seus carros para avisar sobre possíveis colisões. As conquistas das redes neurais convolucionais em problemas de visão foram acompanhadas de aprimoramento parecido das redes recorrentes em problemas de linguagem” (*Ibid.*, p. 239).

possível o progresso da IA. Há, então, uma relação de dependência entre a IA e o modelo de capitalismo de vigilância. Todavia, nesse modelo de negócio, encontra-se o consumidor, vulnerável e fragilizado diante dos arranjos implementados pelas plataformas no ciberespaço.

A era do capitalismo de vigilância e da inteligência artificial causa grandes tensões no que diz respeito aos direitos dos cidadãos, gerando diversos dilemas para a sociedade. Não se pode esquecer esse aspecto da matéria, nem deixar de considerar os riscos e os possíveis prejuízos decorrentes de decisões automatizadas.

1.2.2 Eficiência *versus* direitos

Uma das dificuldades do debate sobre IA é que as corporações se pautam somente pela lógica da eficiência, o que, no atual contexto político-social, é um mantra. Para a utilização das técnicas acima explicadas, são necessárias grandes quantidades de dados, fornecidos, por sua vez, pelos usuários. Assim, recorrendo a diferentes formas de captação de dados, as plataformas conhecem os seus consumidores como poucos. De fato, além dos *fingerprinting* e *flash cookies* já explicitados, as redes sociais são importantes instrumentos para a datificação das experiências humanas, auxiliando no redirecionamento dos conteúdos promovido pelo *marketing* comportamental.

Sumpter, analisando os estudos de Michal Kosinski, professor da Stanford University Graduate School of Business, mostra como a opção de “curtir” nas redes sociais é extremamente eficaz em obter informações das personalidades dos usuários. O professor de Stanford descobriu que “cada ‘curtida’ fornece um pouco de informação sobre uma pessoa e que um acúmulo de ‘curtidas’ permite que seu algoritmo faça conclusões confiáveis”¹³⁷. Para tanto, o pesquisador aplica um método estatístico denominado “Análise de Componentes Principais” para encontrar relações entre categorias, conseguindo, assim, explicar as várias dimensões do ser humano por meio da tecnologia¹³⁸.

Utilizando-se o que os psicólogos chamam teste de *Big Five* ou modelo dos Cinco Grande Fatores, é possível extrair traços da personalidade do conjunto de curtidas. O Facebook pode, por exemplo, prever o QI, as opiniões políticas e a personalidade das pessoas. Os cinco

¹³⁷ SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 38.

¹³⁸ “O ACP é um método estatístico que rotaciona meu conjunto original de 13-dimensionak, em que cada categoria de publicação é uma única dimensão para revelar as relações mais importantes entre as publicações. A primeira componente principal, a relação que faz a correlação mais forte entre os dados, é uma reta que passa, no sentido positivo, pelas dimensões família/parceiro, estilo de vida e amigos, enquanto passa, no sentido negativo, pelas dimensões piadas/memes, políticas/notícias e trabalho” (*Ibid.*, p. 31).

fatores (*Big Five*) são: abertura a novas experiências, conscienciosidade, extroversão, amabilidade (ou simpatia) e neuroticismo (ou instabilidade emocional)¹³⁹.

Ressalta-se que o *Big Five* não é um método utilizado por algoritmos apenas nas redes sociais, é também usado para a triagem de funcionários, como demonstrou Cathy O’Neil; contudo, o teste não é uma representação fiel das personalidades, o que pode gerar danos aos direitos inatos dos indivíduos¹⁴⁰.

Apesar de seu grau de incerteza, especialmente na admissão de funcionários, o teste mostra-se eficaz na classificação geral dos usuários, pois, enquanto navegam pelo ciberespaço, os consumidores vão revelando sua personalidade para as plataformas. Desse modo, há uma contínua exposição em um nível jamais experimentado em comparação com o mundo analógico, e a situação acentua-se porque as máquinas não esquecem detalhes, como os humanos¹⁴¹. O *Facebook*, por exemplo, domina a técnica de reduzir nossas características (dimensões); seu algoritmo, com poucas interações, já consegue obter um retrato do usuário¹⁴². A partir desse retrato, a rede social consegue realizar uma modulação dos comportamentos dos usuários, intensificando ainda mais a vulnerabilidade comportamental que o assédio de consumo provoca. Para melhor compreender essa influência nos comportamentos, é importante demonstrar exemplos dessa prática por meio de pesquisas científicas.

1.2.3 Exemplos de modulação algorítmica: estudos a partir do Facebook

¹³⁹ *Ibid.*, p. 40.

¹⁴⁰ O’NEIL, Cathy. *Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia*. Tradução de Rafael Abraham. Santo André, SP: Editora Rua de Sabão, 2020, p. 165 *et seq.*

¹⁴¹ “Estamos clicando nossa personalidade para dentro do Facebook hora após hora, dia após dia. Carinhas felizes, dedão para cima, ‘curtir’, carinhas tristes e corações. Estamos dizendo ao Facebook quem somos e o que pensamos. Estamos nos revelando para uma rede social num nível de detalhes que normalmente reservamos para os amigos mais próximos. E, ao contrário de nossos amigos – que tendem a esquecer dos detalhes e são tolerantes em relação às conclusões que tiram sobre nós –, o Facebook está sistematicamente armazenando, processando e analisando nosso estado emocional. Ele está rotacionando nossa personalidade em centenas de dimensões, de modo que possa encontrar a direção mais fria e racional para nos analisar” (SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 41).

¹⁴² “Os métodos utilizados pelo Facebook são baseados na aleatoriedade. Rotacionar um milhão de vezes os dados de um milhão de categorias diferentes de curtidas – que foi o método que funcionou relativamente rápido para minhas 15 categorias – leva algum tempo. Por isso, o algoritmo do Facebook começa escolhendo um conjunto aleatório de dimensões com as quais possa nos descrever. O algoritmo avalia, então, o desempenho dessas dimensões aleatórias, permitindo que ele encontre um novo conjunto de dimensões que melhore sua descrição. Depois de apenas algumas poucas iterações, o Facebook consegue ter uma ideia bastante boa dos componentes mais importantes que descrevem os usuários” (SUMPTER, *loc. cit.*).

A IA tem a capacidade de modular os comportamentos dos usuários graças às grandes quantidades de dados obtidos, conseguindo influenciar as decisões individuais¹⁴³, o que gera uma grande preocupação com o agravamento da fragilidade da autodeterminação dos usuários.

As plataformas com seus códigos têm a capacidade de influenciar os seus usuários, ocorrendo a denominada *modulação algorítmica*¹⁴⁴. Essa prática pode ser bem observada em estudos que se basearam no Facebook.

Um exemplo que confirma o poder de modulação do comportamento é o experimento realizado por James Fowler e pesquisadores do *Facebook* para entender se o *post* de amigos pode influenciar outros usuários. Na campanha da eleição para o Congresso americano de 2010, foi mostrada uma mensagem a 60 milhões de usuários do *Facebook* nos EUA. Um grupo recebeu a mensagem com a foto dos amigos que haviam clicado em “Eu votei” e a frase “Eu votei”, enquanto outros receberam apenas o “Eu Votei” sem foto. A pesquisa buscava entender se a natureza social das mensagens contagiava os outros usuários, levantando a hipótese de que, ao ver os rostos de amigos que já haviam votado e ao ter a chance de lhes dizer que estamos com eles, somos encorajados a sair e a votar. O resultado foi que os usuários que viram a mensagem não social (sem a imagem) foram ligeiramente menos propensos a votar do que os usuários que viram seus amigos que haviam votado. A diferença de probabilidade foi de 0,34%. Uma simples mensagem criou, portanto, um *nudge* para diversos eleitores¹⁴⁵.

Outro exemplo que demonstra essa modulação algorítmica por meio do *Facebook* é a pesquisa realizada por Adam Kramer, cientista de dados da companhia, em conjunto com pesquisadores da Cornell University, para analisar o efeito emocional global das mensagens na rede social. O problema da pesquisa era verificar como a remoção de publicações positivas afetaria as publicações que os usuários fariam.

¹⁴³ “They use it to make important decisions about us and to influence the decisions we make for ourselves” (PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press, 2015, p. 4).

¹⁴⁴ “Esse processo é denominado de modulação algorítmica e é um dos tipos de modulação existente. A modulação algorítmica atua por meio do controle do conteúdo, ao prever os gostos dos indivíduos e criar opções de mundos personalizados para eles. O processo de modulação algorítmica tem quatro etapas principais: 1) identificação do indivíduo; 2) formação de um perfil; 3) construção de dispositivos e serviços de vigilância que gerem dados constantes; 4) atuação sobre o indivíduo, por meio da modulação do seu comportamento” (ERMANTRAUT, Victoria. *Locação de algoritmos de inteligência artificial da Microsoft no Brasil: reflexões, dataficação e colonialismo*. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021, p. 173).

¹⁴⁵ “Ao comparar os usuários do Facebook com os registros de eleitores James e seus colegas estimaram que eles tinham criado pelo menos 60.000 novos eleitores como resultado direto de terem visto a mensagem, e pelo menos, um adicional de 280.000 que haviam votado como resultado do contágio social criado pela mensagem” (SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 162).

Os pesquisadores removeram entre 10 e 90% de publicações positivas da linha do tempo de notícias de cerca de 115.000 usuários, mostrando aos usuários mais publicações negativas do que de costume. Foi assim medido o comportamento dos usuários expostos a notícias negativas em comparação com o grupo de controle (que recebeu as mesmas postagens usuais). O resultado do estudo mostrou que o percentual de palavras positivas usadas por pessoas de cujos *feeds* as notícias positivas haviam sido removidas foi um pouco abaixo dos 5,15%, enquanto, no grupo de controle, foi de 5,25%. Em relação às palavras negativas, o resultado foi uma mudança de 0,04%, isto é, a pessoa escreveu uma palavra negativa a mais em um mês¹⁴⁶.

Cathy O’Neil e Sumpter interpretam de maneira diferente os dados obtidos na pesquisa. Para o matemático inglês, a diferença de 0,1% é irrelevante, ele é cético em relação a essa influência nos comportamentos¹⁴⁷. Segundo a PhD em Matemática por Harvard, as evidências mostram que o *feed* manipulado de fato havia alterado os humores dos usuários. Assim, para a autora, “os algoritmos do *Facebook* podem afetar como milhões de pessoas se sentem, e essas pessoas não saberão que isso está acontecendo”¹⁴⁸.

Os autores do artigo concluíram que “estados emocionais podem ser transferidos para outros por contágio emocional, levando-os a experimentar as mesmas emoções que aqueles ao seu redor”. Ainda ressaltaram que os dados corroboram a possibilidade de contágio de emoção pela rede, mesmo que tais manipulações sejam estatisticamente pequenas, pois a manipulação foi operada em uma escala mínima, 0,1% não é, então, desprezível¹⁴⁹.

¹⁴⁶ SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 162-163.

¹⁴⁷ “Para termos uma ideia de quão pequeno um efeito de 0,1% pode ser em termos de publicação no Facebook, suponha que você seja um usuário relativamente ativo que publica cerca de 100 palavras por dia. Uma diminuição de 0,1% significa que, durante os próximos 10 dias, você irá escrever um total global correspondente a uma palavra positiva a menos” (*Ibid.*, p. 163).

¹⁴⁸ O’NEIL, Cathy. *Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia*. Tradução de Rafael Abraham. Santo André, SP: Editora Rua de Sabão, 2020, p. 285.

¹⁴⁹ “Although these data provide, to our knowledge, some of the first experimental evidence to support the controversial claims that emotions can spread throughout a network, the effect sizes from the manipulations are small (as small as $d = 0.001$). These effects nonetheless matter given that the manipulation of the independent variable (presence of emotion in the News Feed) was minimal whereas the dependent variable (people’s emotional expressions) is difficult to influence given the range of daily experiences that influence mood [...]. More importantly, given the massive scale of social networks such as Facebook, even small effects can have large aggregated consequences [...]: For example, the well-documented connection between emotions and physical well-being suggests the importance of these findings for public health. Online messages influence our experience of emotions, which may affect a variety of off-line behaviors. And after all, an effect size of $d = 0.001$ at Facebook’s scale is not negligible: In early 2013, this would have corresponded to hundreds of thousands of emotion expressions in status updates per day” (KRAMER, Adam; GUILLORY, James E.; HANCOCK, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. *In: PNAS Proceedings of the National Academy of Sciences of the United States of America*, v. 111, n. 24, 2014, p. 8790. Disponível em: <https://www.pnas.org/doi/pdf/10.1073/pnas.1320040111>. Acesso em: 27 mar. 2022).

É importante ressaltar que esse estudo suscitou polêmicas, especialmente porque os usuários foram objeto de experimentos sem saber. Não houve um consentimento inequívoco e informado dos consumidores sobre o experimento¹⁵⁰, assim como ocorreu no famoso caso da *Cambridge Analytica*.

O’Neil destaca como a *internet* forneceu aos anunciantes o “maior laboratório que já existiu para pesquisa de consumidor e geração de *leads*”. A autora sustenta que o *feedback* de cada divulgação chega em segundos. Desse modo, cada campanha pode focar as mensagens mais eficientes para alcançar o consumidor na hora certa e com a melhor abordagem possível para levá-lo ao consumo, em um ajuste fino que nunca cessa¹⁵¹.

Há, portanto, um tensionamento no “cabo de guerra da privacidade” entre as empresas privadas e os consumidores em função da realização de experimentos sem a devida autorização, da criação de perfis identificadores dos usuários e de sua utilização para fins comerciais por meio dos seus códigos¹⁵².

Estudos demonstram as preocupações contemporâneas provocadas pelo capitalismo de vigilância e pela utilização maciça de IA: modulação de comportamento, desrespeito ao consentimento, à proteção de dados, aos direitos de informações e à transparência dos consumidores.

1.2.4 A caixa preta dos algoritmos

Qual o método dos algoritmos empregado pela *Amazon* para fazer as recomendações de compra destinadas a seus consumidores? Como os algoritmos do *Google* fazem a lista de *sites* no seu buscador? Como o *Youtube*, o *Facebook*, o *Twitter* e outras plataformas fazem as sugestões de conteúdo para seus usuários? São sugestões ou formas intencionais de influenciar os consumidores das suas plataformas? Os consumidores não sabem – e as plataformas nem querem que saibam.

¹⁵⁰ SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 162.

¹⁵¹ O’NEIL, Cathy. *Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia*. Tradução de Rafael Abraham. Santo André, SP: Editora Rua de Sabão, 2020, p. 120.

¹⁵² “Essa evolução gera novos e significativos contextos. As informações fornecidas pelas pessoas para que obtenham determinados serviços são tais, em quantidade e qualidade, que possibilitam uma série de usos secundários, especialmente lucrativos para os gestores dos sistemas interativos. Estes, elaborando as informações obtidas quando do fornecimento dos serviços, podem ‘criar’ informações novas (perfis de consumo individual e familiar, análises de preferência, informações estatísticas etc., que interessam a outros sujeitos, a quem estas informações podem ser vendidas)” (RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 46).

O que se sabe é que há uma conjunção de cientistas de dados, oriundos das melhores universidades do mundo, e de algoritmos por meio da análise das informações e do monitoramento constante, conforme mostra Sumpter ao entrevistar um funcionário do serviço de *streaming Spotify*. Há, então, uma alquimia entre homem e máquina para as abordagens personalizadas da publicidade comportamental e a sugestão de conteúdos por meio dos códigos¹⁵³. Por exemplo, se um consumidor viajou para o Rio de Janeiro durante uma semana no mês de julho de 2021, a equipe de *marketing* de uma plataforma fará que um anúncio apareça nos *feeds* das redes sociais e *sites* na web um pouco antes de julho de anos seguintes – período em que tipicamente esse consumidor faria sua próxima viagem –, para antecipar seu desejo de viajar¹⁵⁴.

Para que essa alquimia seja possível, é necessário classificar os usuários em tipos de consumidores com base nos bancos de dados comportamentais: por exemplo, “jovem poupador” ou “jovem consumista”, “idoso com rentabilidade” ou “idoso sem rentabilidade”¹⁵⁵. As classificações são em “baldes”, isto é, em “pessoas como você”¹⁵⁶, podendo resultar em diversas injustiças para os consumidores. Desse modo, o consumidor não é julgado individualmente; está em um grupo em que foi colocado pelo algoritmo, que não respeita as nuances pessoais. Se um número significativo dessas pessoas “semelhantes” se revelar caloteiro ou, pior, criminoso, aquele indivíduo será tratado de acordo com essa classificação¹⁵⁷.

É dessa lógica de pessoas que surgiu o “também gostamos”. A *Amazon* foi a pioneira em explorar essa perspectiva ao apresentar ao consumidor o “relacionado aos itens visualizados” e “clientes que compraram esse item também compraram”. Segundo Sumpter, o fundador da empresa, Jeff Bezos, foi a primeira pessoa a reconhecer que os consumidores desejam ter um número pequeno de escolhas ao navegar na *internet*¹⁵⁸. Aproveitou-se de um *insight* da economia comportamental, pois, como ensina Richard Thaler ao analisar planos de

¹⁵³ “Glenn me disse que o processo de fazer recomendações está longe de ser ciência pura, ‘metade do meu trabalho é tentar descobrir quais respostas geradas por computador fazem sentido’. Quando Glenn escolheu o título de seu trabalho, ele pediu para ser chamado de ‘alquimista de dados’ em vez ‘de cientista de dados’. Ele encara seu trabalho não como uma procura por verdades absolutas sobre estilos musicais, mas como uma classificação que faça sentido para as pessoas. Esse processo requer que humanos e computadores trabalhem juntos” (SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 82).

¹⁵⁴ *Ibid.*, p. 83.

¹⁵⁵ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 60-61.

¹⁵⁶ O’NEIL, Cathy. *Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia*. Tradução de Rafael Abraham. Santo André, SP: Editora Rua de Sabão, 2020, p. 226.

¹⁵⁷ O’NEIL, *loc. cit.*

¹⁵⁸ SUMPTER, *loc. cit.*, p. 113-114.

aposentadoria nos EUA, os indivíduos são procrastinadores por natureza¹⁵⁹. Sumpter confirma esse entendimento ao conversar com uma pesquisadora do Instituto de Ciência de Informação da Universidade da Carolina do Sul¹⁶⁰.

Assim, a partir do *insight* do seu fundador, a *Amazon*, após a análise dos dados comportamentais do grupo de consumo em que um dado usuário foi inserido pelos códigos, envia sugestões de livros, por exemplo. Sumpter afirma que “essas sugestões dão uma ilusão de escolha, mas os livros foram agrupados de acordo com o algoritmo da *Amazon*”. Na realidade, as sugestões são fornecidas após o algoritmo analisar o fato de que outras pessoas que gostam dos mesmos livros fizeram escolhas parecidas com a que o consumidor em questão poderia fazer. Trata-se de uma abordagem probabilística¹⁶¹.

Em determinadas situações, como as sugestões de livros, a problemática não é tão sensível. Contudo, esse contexto pode mudar radicalmente quando se leva em consideração que os consumidores são classificados em grupos de “como você” por planos de saúde e seguradoras, o que torna o problema bem mais delicado¹⁶².

A questão é que os códigos padecem de opacidade, isto é, são incompreensíveis em razão da falta de *accountability* das plataformas, principalmente no que tange à transparência e à responsabilidade. Como argumenta Frank Pasquale, as plataformas estão protegidas por leis de patentes e de propriedade intelectual, enquanto a vida dos consumidores é um livro aberto.

¹⁵⁹ “O primeiro obstáculo é a inércia. Pesquisas revelam que a maioria das pessoas que pagam planos de aposentadoria pensam que deveriam estar poupando mais, e planejam tomar alguma atitude, hum... em breve. Mas então procrastinam e nunca chegam a alterar suas taxas de poupança. Na verdade, a maioria dos participantes de planos raramente faz qualquer mudança nas suas opções de poupança, a menos que mudem de empregos e sejam confrontados com um novo conjunto de formulários que terão de preencher” (THALER, Richard. *Misbehaving: a construção da economia comportamental*. Rio de Janeiro: Intrínseca, 2019, p. 325). Nesse mesmo sentido: “Some nudges work because they inform people; other nudges work because they make certain choices easier; still other nudges work because of the power of inertia and procrastination” (SUNSTEIN, Cass R. *The Ethics of Nudging*. *Yale Journal on Regulation*, [s.l.], v. 32, n. 2, 2015, p. 417. Disponível em: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/8225/15_32YaleJonReg413_2015_.pdf?sequence=2&isAllowed=y. Acesso em: 25 nov. 2021).

¹⁶⁰ “Kristina Lerman, uma pesquisadora do Instituto de Ciência de Informação da Universidade da Carolina do Sul, me disse que nossos cérebros adoram ‘também gostando’. Ela usa um princípio básico para modelar os comportamos on-line. Ela me disse: ‘basicamente, se você pressupõe que as pessoas são preguiçosas, então você consegue prever a maior parte do seu comportamento’” (SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019, p. 116).

¹⁶¹ *Ibid.*, p. 114.

¹⁶² “Consider the plight of Walter and Paula Shelton, a Louisiana couple who sought health insurance. Humana, a large insurer based in Kentucky, refused to insure them based on Paula’s prescription history – occasional use of an antidepressant as a sleep aid and a blood pressure medication to relieve swelling in her ankles. The Sheltons couldn’t get insurance from other carriers, either” (PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press, 2015, p. 27).

Assim, a única dúvida que resta é saber quando esses dados estarão disponíveis e por quanto tempo¹⁶³.

Com efeito, Pasquale considera esses algoritmos como uma caixa-preta, palavra que tem dois significados: “Pode se referir a um dispositivo de gravação, como os sistemas de monitoramento de dados em aviões, trens e carros. Ou pode significar um sistema cujo funcionamento é misterioso; podemos observar suas entradas e saídas, mas não podemos dizer como um se torna o outro”¹⁶⁴.

Dessa maneira, nesse cenário de vigília constante exercida por corporações, os usuários não têm ideia do alcance dessas informações, nem de suas consequências.

Para Pasquale, os perfis de consumo têm uma profundidade e uma especificidade sem precedentes. Essas classificações e *rankings* são utilizados em importantes situações da vida humana, como avaliação de crédito e criação de *scores* para o cálculo de riscos e outros fins. Além disso, os métodos de avaliação também são complexos e protegidos por uma legião de engenheiros e advogados superespecializados¹⁶⁵.

Pode-se dizer que atualmente se vive em uma *sociedade dos scores*. Tais avaliações são realizadas pela IA, e com o *Big Other* são tantos bancos de dados classificadores dos usuários que essa difusão de informações representa riscos para os seus titulares. Agrava-se essa conjuntura com a percepção de que esses bancos são poucos escrutinados¹⁶⁶, o que pode resultar em discriminações ou avaliações errôneas.

Pasquale explora três estratégias críticas para que as plataformas mantenham suas caixas-pretas: “*real*” *secrecy*, *legal secrecy*, and *obfuscations*¹⁶⁷. O sigilo real estabelece uma barreira entre um acesso autorizado e um não autorizado, como uma senha das contas pessoais dos usuários. O sigilo legal diz respeito à obrigação de tornar secretas certas informações—normalmente patentes, por meio de leis sobre a propriedade intelectual. Uma ofuscação ocorre quando há tentativas deliberadas de manter um segredo oculto. Um exemplo seria o caso de uma firma que é obrigada a responder sobre certa informação e para tanto entrega 30 milhões de páginas de documentos para forçar o investigador a perder tempo e para dificultar a

¹⁶³ “But while powerful businesses, financial institutions, and government agencies hide their actions behind nondisclosure agreements, ‘proprietary methods’, and gag rules, our own lives are increasingly open books. Everything we do online is recorded; the only questions left are to whom the data will be available, and for how long” (PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press, 2015, p. 3).

¹⁶⁴ It can refer to a recording device, like the data-monitoring systems in planes, trains and cars. Or it can mean a system whose workings are mysterious; we can observe its inputs and outputs, but we cannot tell how one becomes the other (PASQUALE, *Ibid.*, p. 3)

¹⁶⁵ *Ibid.*, p. 4-6.

¹⁶⁶ *Ibid.*, p. 25.

¹⁶⁷ *Ibid.*, p. 6.

identificação do solicitado. Essas estratégias resultam em opacidade, isto é, em incompreensão dos procedimentos. Como consequência da opacidade, as proibições legais fazem que ninguém saiba – apenas as próprias empresas – como funcionam as técnicas empregadas. Daí a necessidade de transparência nesses procedimentos e, principalmente, de regulamentação¹⁶⁸.

Assim como Pasquale, O’Neil considera que a opacidade dos sistemas automatizados sobre as decisões das máquinas constitui um grande problema para a sociedade, tornando essas programações armas de destruição em massa. O’Neil destaca que os elementos que compõem um algoritmo de destruição em massa são: opacidade, escala e dano¹⁶⁹.

Para O’Neil, os códigos refletem objetivos e certas ideologias dos seus criadores¹⁷⁰. É, então, incorreto presumir que todos os resultados de uma IA são precisos. Logo, a imagem de neutralidade e de ciência da IA é um mito que deve ser desconstruído em um cenário de opacidade, pois dificulta as reivindicações de maior transparência e regulamentação das máquinas¹⁷¹. Segundo O’Neil, muitos sistemas automatizados não utilizam dados primários, usam indicadores aproximados, que a autora denomina *proxies*¹⁷², diferentemente dos modelos de confiança¹⁷³. Portanto, além da escuridão sobre os processos, os dados não são sempre exatos.

Um fator fundamental na técnica do *machine learning* não é a quantidade, é a qualidade dos dados inseridos no *input*. O programador assume uma grande responsabilidade ao tratar os dados coletados no momento de compartilhá-los com a IA¹⁷⁴. Além disso, os dados são padrões

¹⁶⁸ PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press, 2015, p. 8.

¹⁶⁹ O’NEIL, Cathy. *Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia*. Tradução de Rafael Abraham. Santo André, SP: Editora Rua de Sabão, 2020, p. 49.

¹⁷⁰ “Os pontos cegos de um modelo refletem o julgamento e prioridades de seus criadores. Ainda que as escolhas no Google Maps e nos softwares de aviação pareçam claras e inequívocas, outras são problemáticas. O modelo de valor agregado nas escolas de Washington, D.C., avalia os professores basicamente com as notas das provas dos alunos, à medida que ignora quanto os professores os envolvem e cativam, trabalham em tarefas específicas, lidam com o controle da sala ou os ajudam com problemas pessoais ou familiares. É por demais simples, sacrificando a precisão e critério em troca de eficiência [...] Aqui vemos que os modelos, apesar de sua reputação de imparcialidade, refletem objetivos e ideologias” (*Ibid.*, p. 34-35).

¹⁷¹ “Although internet giants say their algorithms are scientific and neutral tools, it is very difficult to verify those claims” (PASQUALE, *op. cit.*, p. 14).

¹⁷² “Eles traçam correlações estatísticas entre o CEP residencial de alguém ou padrões de linguagem e seu potencial de pagar um empréstimo ou conseguir dar conta de um emprego. Essas correlações são discriminatórias e, algumas delas, ilegais. Os modelos de beisebol, em geral, não usam proxies porque usam entradas pertinentes como bolas, strikes e acertos” (O’NEIL, *op. cit.*, p. 29).

¹⁷³ *Ibid.*, p. 30.

¹⁷⁴ CORVALÁN, Juan Gustavo. Inteligencia Artificial GPT-3, PretorIA y Oráculos Algorítmicos en el Derecho. *International Journal of Digital Law*, Belo Horizonte, ano 1, n. 1, jan./abr. 2020, p. 20.

de informações pretéritas da nossa sociedade, marcada por desigualdades e práticas discriminatórias, o que faz com que as máquinas reproduzam esses tipos de comportamento¹⁷⁵.

A pesquisadora Joy Buolamwini, doutoranda no Instituto de Tecnologia de Massachusetts, comprovou que sistemas de inteligência artificial utilizados na análise facial padecem de vieses de gênero e de raça: rostos de peles escuras e de mulheres não são reconhecidos na mesma medida que homens brancos¹⁷⁶. A maioria dos bancos de dados de imagem provém de países como Estados Unidos, Reino Unido, França, Espanha, o que corrobora a limitação desses sistemas para promover a diversidade¹⁷⁷.

Uma das possíveis explicações para as injustiças de raça e de gênero dos códigos é o fato de a função de programação ser predominantemente exercida por homens brancos, havendo uma taxa ínfima de negros e mulheres nessa área¹⁷⁸. Isso pode ser observado no relatório da Organização Internacional do Trabalho (OIT) que aponta os desafios enfrentados pela mulher para ingressar no mercado de programadores: apenas 1 em cada 62 entrevistados era do sexo feminino, o que reflete a segregação ocupacional no setor de Tecnologia da Informação (TI)¹⁷⁹.

Para Bruno Miragem, a inexistência e as possíveis discriminações são os grandes desafios regulatórios do direito do consumidor em relação às decisões automatizadas que existem nas relações consumeristas. Afirma o autor: “É pressuposto da utilização da inteligência artificial no tratamento de dados, sua conformidade com a legislação de proteção dos dados pessoais, em especial respeitando a finalidade do tratamento e a proibição de discriminação ilícita”¹⁸⁰.

¹⁷⁵ NUNES, Dierle; MARQUES, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. *Revista de Processo*, São Paulo, v. 43, n. 285, nov. 2018, p. 425.

¹⁷⁶ BUOLAMWINI, Joy. Artificial Intelligence Has a Problem With Gender and Racial Bias. Here’s How to Solve It. *Time*, Feb, 7, 2019. Disponível em: <https://time.com/5520558/artificial-intelligence-racial-gender-bias/>. Acesso em: 15 mar. 2022.

¹⁷⁷ “Levantamento sobre a Open Images e a ImageNet mediu em quais países foram produzidas as imagens que continham registro de localização. As imagens na Open Images provinham dos Estados Unidos (32,1%), Reino Unido (12,9%), França (4,3%), Espanha (4,1%) e Canadá (3,7%). Por sua vez, a ImageNet esteve ainda mais concentrada: Estados Unidos (45,4%), Reino Unido (7,6%), Itália (6,2%), Canadá (3%) e Austrália (2,8%)” (SILVA, Tarcízio. Colonialidade difusa no aprendizado de máquina: camadas de opacidade algorítmica na Imagenet. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021, p. 93).

¹⁷⁸ *Ibid.*

¹⁷⁹ ILO. *World Employment and Social Outlook: The role of digital labour platforms in transforming the world of work*. Geneva: ILO, 2021, p. 137. Disponível em: https://www.ilo.org/wcmsp5/groups/public/@dgreports/@dcomm/@publ/documents/publication/wcms_771749.pdf. Acesso em: 28 jun. 2021.

¹⁸⁰ MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. *Revista de Direito do Consumidor*, São Paulo, v. 125, ano 28, 2019, p. 42. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1243/1168>. Acesso em: 9 abr. 2022.

Portanto, as máquinas postas no mercado nacional devem estar em conformidade com os preceitos da legislação consumerista e da LGPD.

Em um ambiente que se importa apenas com a quantidade e não pela qualidade de dados, não existe uma mensuração de igualdade no *opt in*, desse modo, não há um tratamento para que os dados compartilhados não correspondam apenas a homens brancos, como no caso apontado por Joy Buolamwini. Isso faz com que a utilização de algoritmo se torne um risco na tomada de decisões, por reforçar injustiças na sociedade. Além disso, como será exposto, há violações de direitos constitucionais, como o contraditório e o devido processo legal, pois as plataformas agem unilateralmente por meio dos algoritmos.

Dessa forma, cria-se uma conjuntura em que não se conhecem as premissas da máquina para chegar a um dado resultado, o que gera uma grande assimetria informacional entre usuários e *players*, resultando em uma vulnerabilidade algorítmica, que será abordada em conjunto com as demais vulnerabilidades que o consumidor enfrenta no ciberespaço.

1.2.5 A necessidade de adequar o direito às novas realidades sociais

A complexidade das relações tecnológicas fragiliza a proteção do consumidor de maneira sem precedentes. Para lidar com um problema, é necessário primeiro identificar seus atores, seus procedimentos e suas nuances. Lançar luz é esclarecer as dificuldades e os riscos enfrentados em determinada circunstância, pois, como bem afirma Brandeis, “a luz do sol é o melhor dos desinfetantes”.

Para se compreender a questão da proteção de dados, é vital conhecer a conjuntura vivenciada. Este capítulo trata o contexto como ele é, de forma pragmática. Apresentam-se conceitos que são importantes para o desenvolvimento do trabalho, para que, assim, o leitor saiba os sentidos assumidos pelos termos na abordagem da problemática referente à proteção de dados pessoais dos consumidores no ciberespaço.

Ao tratar da revolução tecnológica, especialmente no que tange ao objeto deste trabalho – *internet*, comércio digital e dados –, busca-se demonstrar como se deu essa revolução e as transformações por ela provocadas. É importante conhecer o novo modelo de negócio consolidado na *internet*, as plataformas, para entender como essa *internet* participativa (*web 2.0*) impulsionou a relação dos usuários com os fornecedores, que resultou na descoberta do denominado superávit comportamental.

O superávit de comportamento permitiu às plataformas abordagens personalizadas por meio da publicidade direcionada, o que representou uma grande evolução para o *marketing*. A

ciência mercadológica, aproveitando-se do *Big Data*, tornou-se a principal fonte de renda dos capitalistas de vigilância. Esse modelo de negócio criado na *internet* não é um desenvolvimento inevitável das evoluções tecnológicas; na realidade, é o resultado de escolhas que visaram a melhor maneira de monetizar os novos serviços tecnológicos.

Como sustenta Zuboff, o neoliberalismo apresenta-se como a lógica que direciona as práticas e os métodos das empresas, mostrando-se indispensável para os objetivos das grandes companhias tecnológicas, especialmente no que diz respeito à aversão à regulamentação e à veneração da autorregulamentação. Como visto, a regulamentação dessas atividades enfrenta diversas dificuldades, sendo as mais sensíveis o não acesso às informações sobre os órgãos reguladores em razão das práticas institucionalizadas de *real secrecy*, *legal secrecy* e *obfuscation*, as diferentes velocidades entre a criação tecnológica e as respostas dos Estados e a assimetria de poder entre as grandes plataformas e os consumidores e reguladores.

Desse modo, as tecnologias de ponta, como a inteligência artificial, são utilizadas todos os dias nos novos serviços tecnológicos, classificando consumidores e predizendo suas ações, inclusive tendo em vista a modulação algorítmica dos comportamentos. Tais tecnologias são inescrutáveis pela sociedade, enquanto o consumidor encontra-se translúcido no ciberespaço, o que resulta em uma assimetria sem igual de poder e de informação. Verifica-se, ainda, que os sistemas automatizados são caixas-pretas para os órgãos reguladores e a sociedade, padecendo de opacidade. Acentua-se esse cenário com as comprovações de injustiças automatizadas em campos sensíveis para a vida de um consumidor, como na admissão em um plano de saúde, que pode ser negada pelo prestador se a pessoa usou antidepressivos¹⁸¹, ou na concessão de empréstimos e seguros com melhores taxas, como demonstra O’Neil.

Em razão dessas questões e à luz dos ensinamentos de Pasquale, entende-se que se deve aprofundar a interpretação das leis referentes às questões tecnológicas, como a proteção de dados pessoais dos consumidores. Constatou-se que a criação de leis para regular especificamente certos modelos de negócios não se mostrou eficiente, como pode ser observado no exemplo brasileiro do Decreto n.º 7.962/2013, que, em seu artigo 3.º, regulou as “compras coletivas”¹⁸². Na época, era um modelo de negócio que interessava aos consumidores, com

¹⁸¹ PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press, 2015, p. 26.

¹⁸² BRASIL. Decreto n.º 7.962, de 15 de março de 2013. Regulamenta a Lei n.º 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. *Diário Oficial da União*: seção 1, Brasília, DF, edição extra, p. 1, 15 mar. 2013. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2013/decreto-7962-15-marco-2013-775557-publicacaooriginal-139266-pe.html>. Acesso em: 14 jan. 2022.

empresas como Peixe Urbano, contudo, esse modelo de negócio inexistia atualmente. Peixe Urbano, em 2021, retirou seu *site* do ar e deixou de pagar seus funcionários¹⁸³.

Portanto, é primordial estender interpretações e fortalecer princípios, como o da confiança, o da informação e o da finalidade, para enfrentar as dificuldades impostas pelo B2C.

O direito como ciência jurídica tem o dever de se adequar aos novos movimentos da sociedade tecnológica, principalmente quando as mudanças representam riscos difusos e geram danos aos consumidores. O direito privado tem a função de proteger a pessoa contra os desafios da revolução tecnológica, entendendo o consumidor a partir da sua vulnerabilidade¹⁸⁴. Importa também reconhecer que a proteção do consumidor no ordenamento jurídico, além de ser a proteção de um direito fundamental (CF, art. 5.º, XXXII), é um pilar da ordem econômica, conforme preceitua o artigo 170, V, da CF.

Como Claudia Marques e Bruno Miragem apontam, o direito privado deve ser concebido com base no pluralismo de fontes nacionais e internacionais existentes, realizando um diálogo entre as fontes para garantir a melhor proteção do consumidor¹⁸⁵ em tempos de serviços de tamanha complexidade – cujas implicações são entendidas somente pelas plataformas.

Cabe à ciência jurídica reexaminar as normas e os princípios das legislações para buscar novas formas de interpretação que deem conta do problema causado pela evolução tecnológica a direitos e garantias fundamentais. Ensina Miragem: “Resta ao jurista que se debruça sobre o fenômeno conciliar visões perspectiva e prospectiva sobre as repercussões do direito sobre a realidade que se impõe neste novo mercado de consumo”¹⁸⁶:

Em razão de todas as assimetrias na relação entre usuários e *players*, é vital buscar interpretações mais favoráveis e protetivas para os consumidores, protegendo suas legítimas expectativas com os serviços ofertados, especialmente *suas legítimas expectativas de proteção de dados*.

¹⁸³ KNOTH, Pedro. Após ‘febre’ da compra coletiva, Peixe Urbano tem crise e está fora do ar. *Uol Economia*, 20 maio 2021. Disponível em: <https://economia.uol.com.br/noticias/redacao/2021/05/20/como-o-peixe-urbano-foi-de-queridinho-a-alvo-de-reclamacoes-em-uma-decada.htm>. Acesso em: 2 abr. 2022.

¹⁸⁴ FACHIN, Luiz Edson; SILVA, Roberta Zumblick Martins da. Direito do consumidor, novas tecnologias e inclusão digital. *Revista de Direito do Consumidor*, São Paulo, n. 139, ano 31, jan./fev. 2022, p. 21-22.

¹⁸⁵ MARQUES, Claudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. São Paulo: Revista dos Tribunais, 2014, p. 196-197.

¹⁸⁶ MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. *Revista de Direito do Consumidor*, São Paulo, v. 125, ano 28, 2019, p. 58. Disponível em: <https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1243/1168>. Acesso em: 9 abr. 2022.

2 A PROTEÇÃO DE DADOS PESSOAIS COMO UM DIREITO FUNDAMENTAL E A TEORIA DA CONFIANÇA NO DIREITO PRIVADO

2.1 A PROTEÇÃO DE DADOS PESSOAIS E SEUS FUNDAMENTOS

A proteção de dados, para alcançar o *status* de direito fundamental em diversos países, como no Brasil, passou por um longo caminho. Para entender o desenvolvimento da disciplina e da sua importância ao longo do tempo, é necessário rever seus fundamentos: os direitos da personalidade e da privacidade.

O desenvolvimento dos fundamentos da proteção de dados dá-se por meio de discussões doutrinárias no âmbito do movimento da despatrimonialização do direito privado. Após a Segunda Guerra Mundial e com o advento do Estado Social, os estudos de Direito Constitucional na Europa alcançaram grande força, visando a reconstrução da concepção de direitos fundamentais. Impunha-se uma nova leitura ante as novas necessidades emancipatórias dos cidadãos¹⁸⁷.

O movimento em prol da codificação, ocorrido no século XIX na Europa a partir da experiência do Código de Napoleão, caracterizou-se por encampar os interesses da burguesia, protegendo a autonomia contratual nos negócios jurídicos e a propriedade, conferindo maior segurança às negociações¹⁸⁸. Nesse momento, os códigos buscavam proteger direitos que possuíam carga patrimonialista. Assim, direitos como os da personalidade e da privacidade não tinham espaço no ordenamento jurídico, especialmente em razão da força do Positivismo na época¹⁸⁹.

Somente a partir do fim da Segunda Guerra Mundial, com a difusão do princípio da dignidade humana nas constituições, direitos e interesses existenciais individuais começam a ocupar o centro dos debates.

Nesse momento, fala-se na despatrimonialização do direito civil, focando-se a tutela jurídica do ser humano, colocando o indivíduo no centro das legislações. É nesse contexto que se desenvolvem direitos como o da personalidade e o da privacidade, quando o movimento de

¹⁸⁷ SARMENTO, Daniel. *Direitos fundamentais e relações privadas*. 2. ed., 3. tir. Rio de Janeiro: Lumen Juris, 2010, p. 130.

¹⁸⁸ *Ibid.*, p. 93.

¹⁸⁹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 48.

codificação perde força para a instituição das Constituições com valores e princípios humanísticos¹⁹⁰.

Na Constituição brasileira, o princípio da dignidade da pessoa humana (art. 1, III) é reconhecido como um princípio político-constitucional¹⁹¹. Nesse sentido, considera-se a dignidade da pessoa humana como um valor absoluto do homem, que se irradia por todo o ordenamento de Estados Democráticos de Direito porque é um bem jurídico que goza de proteção por ser inato a todos os seres humanos. Para Maria Bodin de Moraes, esse princípio visa garantir o respeito e a proteção da dignidade, mas, além disso, é um valor ético-jurídico fornecido pela democracia, gerando uma transformação no Direito Civil, considerando que os valores da codificação não são mais seus fundamentos axiológicos¹⁹².

É nesse contexto que se firmam os fundamentos da proteção de dados, que se inserem entre os direitos de privacidade e de personalidade. Logo, é importante entender a proteção de dados como fruto da evolução desses dois direitos fundamentais¹⁹³. É essencial examinar os fundamentos da proteção de dados pessoais para compreender a importância da disciplina como um direito fundamental no ordenamento jurídico nacional.

2.1.1 O direito à privacidade

Um espaço seguro, livre de intromissões e de pressões sociais é perseguido pela humanidade há séculos. Na Grécia Antiga, a título de exemplo, havia santuários considerados um ambiente sagrado com a finalidade de asilo ou de sacrifício religioso. A palavra grega *asylon* significa “lugar inexpugnável”, tratava-se, pois, de um espaço inviolável. Na era moderna, a ideia de inviolabilidade das relações íntimas vinculadas outrora à lei de asilo ressurgiu com as proteções constitucionais e declarações de direitos inalienáveis a partir do *common law*¹⁹⁴.

¹⁹⁰ SARMENTO, Daniel. *Direitos fundamentais e relações privadas*. 2. ed., 3. tir. Rio de Janeiro: Lumen Juris, 2010, p. 100-101.

¹⁹¹ “O princípio da dignidade da pessoa humana (art. 1, III, da CF) enquadra-se na categoria de princípio político constitucional. Ele elenca, conforme observado, uma das opções político-constitucionais do legislador constituinte” (BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor*. São Paulo: Almedina, 2019, p. 19).

¹⁹² MORAES, Maria Celina Bodin de. Danos à pessoa humana: uma leitura civil-constitucional dos danos morais. In: SARLET, Ingo Wolfgang (org.). *Constituição, direitos fundamentais e direito privado*. 2. ed. Porto Alegre: Livraria do Advogado, 2006, p. 74.

¹⁹³ SARMENTO, *op. cit.*, p. 48.

¹⁹⁴ “O *common law* [direito comum] inglês manteve a ideia do castelo como fortaleza inviolável e a converteu para a concepção mais abrangente de ‘lar’, um santuário livre de intrusões arbitrárias: inexpugnável. A longa linha do privilégio de santuário reapareceu na jurisprudência americana. Em um texto de 1995, a estudiosa do direito Linda McClain argumentou que a equiparação de lar como santuário dependeu menos da santidade dos direitos de propriedade do que um compromisso com as ‘privacidades da vida’. Segundo ela, ‘há um forte tema de um reino apropriado de inacessibilidade ou segredo com respeito ao mundo como um todo, bem como um

O desenvolvimento do direito à privacidade como se conhece ocorre apenas no século XX. De fato, apesar do movimento em favor da despatrimonialização, a privacidade não foi reconhecida nas Constituições, nem nos Códigos Civis do século XIX. Seu desenvolvimento decorre de debates doutrinários em função do surgimento de novos instrumentos tecnológicos que começavam a impactar a vida cotidiana dos cidadãos¹⁹⁵.

O seminal artigo “The Right to Privacy”, de Warren e Brandeis, inicia a discussão sobre as influências das tecnologias da época na vida privada. Naquela época, tratava-se das câmeras fotográficas e dos jornais que começavam a interferir na vida doméstica; foram o ponto de partida para o entendimento contemporâneo da privacidade. Os autores buscam identificar uma proteção para esse direito com base no *common law*. Segundo eles, esse sistema jurídico possui a característica de ser dinâmico, logo, é possível ampliar seu escopo de proteção para outros direitos ainda não assegurados, como o da privacidade¹⁹⁶.

Para Warren e Brandeis, então advogados, as recentes invenções e métodos corporativos suscitavam a necessidade de proteger a pessoa, garantindo a segurança do indivíduo. À luz desse entendimento, os autores defendem o direito de ser deixado só (*the right to be alone*), um conceito criado pelo juiz Cooley, em 1888, dois anos antes da publicação do artigo. O escrito é fundamental para entender como se iniciou a epistemologia do direito à privacidade: ligado à dicotomia entre o público e o privado¹⁹⁷.

Historicamente o direito à privacidade advém da diferenciação entre público e privado, entre sigilo e transparência. Assim, se um indivíduo se encontra em um espaço público, ele está sujeito ao escrutínio; todavia, se esse mesmo indivíduo se encontra em um espaço privado, como seu lar, ele estará protegido de qualquer interferência, tendo o direito de ser deixado só, em uma espécie de refúgio¹⁹⁸.

Nesse sentido, Rodotà atribui inicialmente à privacidade um forte componente individualista. Para o autor, esse direito é burguês, pois a privacidade estaria associada ao fim

reconhecimento da importante dimensão social de tal espaço interno protegido [...]” (ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 538-539).

¹⁹⁵ MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 14. Disponível em: <https://repositorio.unb.br/handle/10482/4782>. Acesso em: 11 abr. 2022.

¹⁹⁶ “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops’” (WARREN, Samuel D.; BRANDEIS, Louis D. *The Right to Privacy*. *Harvard Law Review*, v. 4, n. 5, Dec. 1890, p. 195. Disponível em: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 22 jan. 2022).

¹⁹⁷ WARREN; BRANDEIS, *loc. cit.*

¹⁹⁸ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 91.

da sociedade feudal. Com a desagregação do feudalismo, a intimidade era possível somente para aqueles que dispunham de meios materiais para o seu exercício, visto que o isolamento era um privilégio de pouquíssimos eleitos que poderiam viver longe da comunidade. Dessa maneira, para o autor, a privacidade é uma possibilidade da classe burguesa, que “consegue realizá-la sobretudo graças às transformações socioeconômicas relacionadas à Revolução Industrial”¹⁹⁹. Embora Rodotà faça a ressalva de que é errado considerar a privacidade apenas em relação à burguesia, ele reconhece que a degradação das condições de vida dessa classe faz com que esse direito se degrade²⁰⁰. Constata-se, portanto, a importância da existência de alicerces estruturais para o exercício desse direito.

Nessa esteira, Albert Bendich, no artigo “*Privacy, Poverty and the Constitution*”, afirma que privacidade e pobreza estão intimamente e inversamente relacionadas²⁰¹. A prática de aproveitar a própria intimidade, seja em um refúgio na cidade, seja na ideia do *fugere urbem*, é um privilégio de uma classe social; nesse contexto, o direito à privacidade liga-se ao direito de propriedade, pois, em uma perspectiva solitária e patrimonial, é necessário ter um espaço seu para dele se apropriar.

Essa visão transparece no artigo 5.º, XI, da Constituição Federal, que dispõe: “a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante ou desastre ou para prestar socorro, ou, durante o dia, por determinação judicial”.

Uma grande contribuição do artigo de Warren e Brandeis foi romper com a visão da privacidade ligada à propriedade. Os autores, ao defenderem o direito de privacidade, relacionam esse direito com o livre desenvolvimento da personalidade do indivíduo, visto que a privacidade é um valor humano extremamente valioso. Portanto, como bem destaca Laura Mendes, a importância desse artigo não reside apenas na identificação do direito de privacidade,

¹⁹⁹ RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 26.

²⁰⁰ “Naturalmente, também seria errado considerar a privacidade de forma monolítica em relação à própria classe burguesa: a privacidade, por exemplo, destina-se a desaparecer onde se degradam as condições de vida dessa classe, como ocorre na pequena burguesia europeia confinada em habitações populares [*alveari*] na periferia das grandes cidades. Da mesma forma, não pode ser desconsiderado o fato de que esse modelo cultural tende a ser importado pelos estratos mais altos da classe operária” (*Ibid.*, p. 28).

²⁰¹ “As a matter of abstract consideration, it seems clear that poverty and privacy are intimately and inversely related. If the essence of the right to privacy is in that pattern of rights making for meaningful freedom of choice in the context of our society, it requires little reflection to perceive that nutritional or cultural starvation constitutes a form of compulsion or constraint rather incompatible with such freedom” (BENDICH, Albert M. *Privacy, Poverty and the Constitution*. *California Law Review*, Berkeley, v. 54, n. 2, 1966. p. 414. Disponível em: <https://lawcat.berkeley.edu/record/1110014>. Acesso em: 11 abr. 2022).

mas também na fundamentação atribuída a esse direito, relacionando-o à inviolabilidade da personalidade²⁰².

Entendendo a privacidade como um instrumento de garantia do livre desenvolvimento de um indivíduo na sociedade, Bendich argumenta que o exercício da privacidade pressupõe alicerces, pois, se a essência do direito de privacidade está na garantia de se autodeterminar, a fome ou a falta de moradia, por exemplo, constituem restrições sérias ao exercício da privacidade²⁰³. Nessa esteira, a privacidade é um direito que possibilita o exercício de diversas garantias constitucionais, como a liberdade de expressão, a liberdade de pensamento, a possibilidade de se autodeterminar, o direito de não ser discriminado e outros.

Como bem salienta Bioni, fazendo referência a Hannah Arendt, a privacidade é um princípio não apenas humano, mas também da democracia. É por meio da privacidade que surgem pensamentos críticos, o refúgio representa um ambiente para visões divergentes, livres da pressão social²⁰⁴. Nesse mesmo sentido, Bendich vê na privacidade uma relação intrínseca com a ideia de liberdade e de dignidade, garantindo uma natureza independente de espírito e pensamento²⁰⁵. Orwell, em *1984*, conseguiu expressar como ninguém a angústia de se viver em uma sociedade sem privacidade e sem possibilidade de livre desenvolvimento da personalidade, bem como seus efeitos nos cidadãos da fictícia Oceania.

Em razão dos valores que exprimem a privacidade, conceber esse valor humano apenas na perspectiva do público e do privado é deficiente e insatisfatório em relação aos anseios da sociedade tecnológica. Portanto, a lógica centrada na liberdade negativa, do direito de ser deixado sozinho de um indivíduo mostra-se fragilizada, sendo necessário buscar novos fundamentos – ainda mais quando se leva em consideração a difícil conceituação do que é público e do que é privado, especialmente no atual contexto de uma sociedade confessional²⁰⁶.

²⁰² MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 14-15. Disponível em: <https://repositorio.unb.br/handle/10482/4782>. Acesso em: 11 abr. 2022.

²⁰³ BENDICH, Albert M. Privacy, Poverty and the Constitution. *California Law Review*, Berkeley, v. 54, n. 2, 1966. p. 414. Disponível em: <https://lawcat.berkeley.edu/record/1110014>. Acesso em: 11 abr. 2022.

²⁰⁴ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 91.

²⁰⁵ “Historically, the right to privacy is intimately tied up with the nurturing of independence of mind and spirit. It is part of the process of civilization struggling to overcome tyranny and oppression. It is related most intimately to the development of the first amendment freedoms: conscience, speech, press, assembly, petition. But, basically, the right to privacy grew up as part of the ongoing struggle for the freedom and dignity of the individual, his right to determine his own destiny, to think and choose for himself, and to join in association with free and equal fellow citizens in shaping and working to reach common social and political ends” (BENDICH, *op. cit.*, p. 408-409).

²⁰⁶ “Vive-se naquilo que Debord chamou de ‘Mundo Invertido’, em que o verdadeiro é apenas um momento do falso [...], pois numa sociedade confessional como a atual, não basta apenas adquirir os mutantes símbolos de consumo da indústria cultural, mas revelar a ‘feliz’ aquisição aos demais, preferencialmente nas redes sociais e

Dessa maneira, a privacidade evoca a necessidade de diferentes entendimentos, pois, com o desenvolvimento da humanidade e a revolução tecnológica, esse direito deixou de ter uma característica apenas burguesa para atingir a coletividade. Com efeito, como explicado no primeiro capítulo, houve uma total imersão dos cidadãos no ciberespaço – e eles são consumidores. Assim, a privacidade supera o tradicional quadro individualista para dilatar-se em uma dimensão coletiva, considerando o indivíduo como pertencente a uma sociedade²⁰⁷. Essa mudança paradigmática – o indivíduo está *dentro* da sociedade – fez surgir uma dimensão positiva da privacidade, abandonando-se a ideia de liberdade negativa de outrora para adotar uma perspectiva de *exercício de controle* que se adapte ao dinamismo do fluxo informacional²⁰⁸.

Nesse mesmo sentido, Rodotà afirma que “coerentemente, com a mudança da própria definição de privacidade a atenção deve passar do sigilo para o controle”. Logo, o novo significado da privacidade nos sistemas contemporâneos é voltado para o problema do controle do fluxo informacional²⁰⁹.

Como se pode observar, as mudanças de perspectiva sobre a privacidade refletem a mudança do direito, que passa a considerar a pessoa no centro gravitacional dos ordenamentos jurídicos. Há, portanto, uma adequação do direito ao contexto histórico de valorização da democracia e da personalidade do indivíduo. Essa capacidade dinâmica do direito fica mais clara com a revolução tecnológica, fazendo com que a visão da privacidade segundo a lógica patrimonialista seja defasada e incoerente com os novos arranjos da sociedade, que clama por mecanismos de controle sobre suas informações.

Em função das novas visões da privacidade, o conceito desse direito gera controvérsia, havendo diversos entendimentos sobre o tema, que envolvem as dimensões da privacidade.

2.1.1.1 Algumas privacidades

condicionar o bem-estar à quantidade de ‘amigos’ virtuais que aprovaram aquele momento” (VERBICARO, Dennis; RODRIGUES, Lays Soares dos Santos. Reflexões sobre o consumo na hipermodernidade: o diagnóstico de uma sociedade confessional. *Revista Direito em Debate*, [s.l.], v. 26, n. 48, jul./dez. 2017, p. 357. Disponível em: <https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/6836>. Acesso em: 15 mar. 2022).

²⁰⁷ RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 29-30.

²⁰⁸ “[...] a esfera privada não seria algo já posto à espera de uma violação, mas um espaço a ser construído a posteriori e dinamicamente mediante o controle das informações pessoais. Haveria, por isso, uma mudança qualitativa representada pela transposição do eixo antes focado no trinômio ‘pessoa-informação-sigilo’ ao eixo agora composto por quatro elementos – ‘pessoa-informação-circulação-controle’” (BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 94)

²⁰⁹ RODOTÀ, *op. cit.*, p. 36-37.

Como se pode observar, diferentes autores têm interpretações e entendimentos distintos sobre a privacidade. Não há uma unanimidade, nem quanto ao conceito jurídico. Procura-se aqui apresentar outros sentidos de privacidade, para além dos já aludidos, ressaltando-se que não há nenhuma pretensão de esgotar as dimensões da privacidade.

O termo “privacidade” é objeto de controvérsia, em razão de sua indefinição conceitual. De qualquer maneira, para Doneda, “essa indefinição deve ser tomada mais como uma característica intrínseca da matéria que como um defeito ou obstáculo”. Cabe lembrar que o vocábulo “privacidade” é de raiz latina, todavia, o desenvolvimento do conceito de privacidade ocorreu na língua inglesa, não havendo como fazer um paralelo com os idiomas latinos²¹⁰.

Desse modo, existe, por exemplo, a ideia da privacidade como o direito de ser deixado sozinho (*right to be alone*), sem interferências indesejadas. Laura Mendes explica os limites que Warren e Brandeis definiram para o conceito no renomado artigo: a) o direito à privacidade não impede a publicação do que é publicado ou do que é de interesse geral; b) o direito à privacidade não veda a comunicação de tudo o que é privado; c) a reparação não será exigível se a intromissão for gerada por uma revelação verbal que não cause danos; d) o consentimento do afetado exclui a violação do direito; e) a alegação de veracidade da informação pelo agressor não exclui a violação do direito; f) a ausência de dolo também não exclui a violação desse direito²¹¹.

Outra perspectiva da privacidade é encontrada na teoria das esferas de Heinrich Hubmann, segundo a qual há várias esferas concêntricas que circundam a vida privada do indivíduo. Sendo assim, a privacidade é compreendida a partir de círculos concêntricos, que representam diferentes graus de privacidade. No núcleo, estaria a esfera da intimidade, do segredo; englobando o núcleo, estaria a esfera privada; acima dessas esferas, encontrar-se-ia a esfera pessoa, que abraçaria a vida pública do indivíduo. Tal doutrina foi objeto de críticas e superada pela própria doutrina alemã por considerar o sujeito como uma pessoa passiva. Segundo Laura Mendes, o artigo 5.º, X, da Constituição Federal, dispositivo que assegura a proteção da privacidade no ordenamento nacional, é embasado na teoria das esferas recorrendo

²¹⁰ “O vocábulo ‘privacidade’, em si, tem raiz latina (o verbo *privare*, cuja forma adjetiva é *privatus*), muito embora hoje a utilizemos em grande parte devido ao seu intenso emprego na língua inglesa – o que faz com que muitos hoje a representem como um anglicismo. De fato, o vigoroso desenvolvimento do termo *privacy* na língua inglesa não teve paralelo em idiomas latinos, ao menos como um substantivo simples – basta mencionar que no século XVI a literatura inglesa já utilizava amplamente o termo” (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2021. *E-book*, cap. 1).

²¹¹ MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 16. Disponível em: <https://repositorio.unb.br/handle/10482/4782>. Acesso em: 11 abr. 2022.

à ideia de vida privada e intimidade. Salienta-se que, embora a norma tenha tipificado esses termos, a distinção não opera efeitos jurídicos na tutela da privacidade no Brasil²¹².

Para Bendich, a privacidade é a proteção do cidadão contra autoridades, é uma garantia individual, o respeito pela integridade individual de cada sujeito, lembrando que o indivíduo está à frente do Estado. Mas o autor ressalta que a proteção da privacidade não é apenas a proteção de direitos individuais, é também a proteção da liberdade por ela mesma em razão do seu aspecto público. Logo, proteger a privacidade é proteger a liberdade em uma sociedade²¹³.

Outra ideia de privacidade importante é a de Alan Westin. O autor identificou uma relação entre privacidade e liberdade, pressupostos fundamentais para a cidadania na democracia, pois o desenvolvimento individual é particularmente importante em sociedades democráticas²¹⁴. Como destaca Doneda, Westin apontou que o aspecto informativo é essencial para o indivíduo e para a sociedade, garantindo liberdades importantes. Assim, Westin levou a discussão da privacidade ao nível da autodeterminação na comunidade²¹⁵.

Nos anos 70, Westin identificou ameaças à privacidade em decorrência da tecnologia, que teriam relação com a vigilância física, a vigilância psicológica e a vigilância de dados pessoais²¹⁶. Por causa dessas intromissões, o autor entende que a privacidade é o direito de controlar a forma como os outros utilizam as informações a nosso respeito. “Privacidade é a reivindicação de indivíduos, grupos ou instituições para determinar, quando, como e em que extensão, informações sobre si próprios devem ser comunicadas a outros”²¹⁷. Contudo, como destaca Mendes, para Westin, a privacidade não é um direito absoluto, havendo limitações individuais e coletivas para seu exercício²¹⁸.

²¹² MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 19-20. Disponível em: <https://repositorio.unb.br/handle/10482/4782>. Acesso em: 11 abr. 2022.

²¹³ “The protection of the right to privacy is therefore not merely a protection of the private rights of individuals, but it is also a protection of a most fundamental aspect of the public interest. It is a protection *of freedom itself*. That is why no infringement of so fundamental a right can be justified on any grounds which might suffice to justify invasions of lesser rights such as property rights. Property rights may be regulated and abridged in the public interest. Privacy, like freedom of speech, is itself an aspect of the public interest” (BENDICH, Albert M. *Privacy, Poverty and the Constitution*. *California Law Review*, Berkeley, v. 54, n. 2, 1966. p. 441, grifo nosso. Disponível em: <https://lawcat.berkeley.edu/record/1110014>. Acesso em: 11 abr. 2022).

²¹⁴ WESTIN, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967, p. 34.

²¹⁵ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2021. *E-book*, cap. 2.

²¹⁶ *Ibid.*, cap. 1.

²¹⁷ WESTIN, *op. cit.*, p. 7.

²¹⁸ MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 23. Disponível em: <https://repositorio.unb.br/handle/10482/4782>. Acesso em: 11 abr. 2022.

Rodotà também compreende a privacidade como “o direito de controlar a própria informação e determinar a forma de construir a própria esfera privada”, sendo o direito à privacidade um direito de controle e de autodeterminação da vida privada²¹⁹. Daniel Solove aponta a dificuldade de conceituar esse direito, mas entende que a privacidade deve ser definida a partir de uma generalidade e analisada a partir do contexto. Essa análise contextual é fundamental, pois o conceito de privacidade é volátil, mudando conforme os comportamentos da população²²⁰.

Nessa esteira, Helen Nissenbaum defende a *privacidade em uma integridade contextual*²²¹. Para a autora, a informação possui um valor social, podendo pertencer a certas arenas da vida, dependendo do contexto. Assim, é necessário confirmar se a integridade do tráfego dos dados pessoais respeita um contexto. Há várias esferas de informações que circulam os indivíduos nos mais variados locais da vida cotidiana. Os indivíduos fazem parte de diversos reinos, os quais seguem suas próprias normas sociais. Para Nissenbaum, existem dois tipos de normas informacionais: normas de adequação (*norms of appropriateness*) e normas de distribuição (*norms of distribution*). Para a autora, “A integridade contextual é mantida quando ambos os tipos de normas são mantidos, e é violada quando qualquer uma das normas é violada”²²².

As normas de adequação (*appropriateness*) determinam qual informação pessoal é apropriada para ser revelada em determinado contexto, ou seja, são normas que versam sobre a natureza da informação. Nissenbaum cita o exemplo da relação entre médico e paciente, na qual é totalmente apropriado partilhar detalhes da saúde (dados sensíveis) com o médico em uma consulta; mas provavelmente, em outro contexto, isso não é apropriado. As normas de distribuição (*distribution*) são aquelas que avaliam o fluxo de informações ou de transferência de informações para um terceiro, aferindo se estavam de acordo com as expectativas do titular. Desse modo, deve-se observar não apenas se as informações são apropriadas ou inadequadas para um dado contexto, mas também se sua distribuição ou seu fluxo respeita normas

²¹⁹ RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 78-80.

²²⁰ SOLOVE, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008, p. 46 *et seq.*

²²¹ NISSENBAUM, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. [S.l.]: Stanford Law Books, 2010.

²²² *Contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated* (NISSENBAUM, Helen. *Privacy as Contextual Integrity*. *Washington Law Review*, [s.l.], v. 79, n. 1, 2004, p. 138)

contextuais do fluxo de informações²²³.

De todas as ideias de privacidade, extrai-se a preocupação com o modo de controlar essas informações para que sejam distribuídas ou reveladas conforme o interesse do indivíduo, não minando seu livre desenvolvimento na sociedade. Verifica-se, então, a existência de uma relação intrínseca entre privacidade e direitos de personalidade, que juntos formam a base da disciplina de dados pessoais como se entende atualmente.

Além disso, é evidente que o conceito de privacidade é dinâmico, assumindo diferentes significados ao longo do seu desenvolvimento. Apesar disso, é evidente sua ligação com o ideal de livre desenvolvimento, no sentido de permitir a liberdade de autodeterminação dos indivíduos. A privacidade é um direito fundamental e constitucional muito importante para a sociedade, sendo importante analisar os direitos de personalidade e seu desenvolvimento.

2.1.1.2 Os direitos de personalidade

Os direitos da personalidade emergiram como categoria autônoma na dogmática civilista no século XIX com o movimento jusnaturalista. Contudo, como salienta Sarmento, houve uma intensa reação da doutrina da época, negando-se a existência desses direitos em função da afirmação de que a personalidade não poderia ser objeto de direito, visto que ela identificava a titularidade de direitos. Contudo, não demorou muito para a personalidade ser concebida sob duas perspectivas: como centro de imputação e pressuposto para a aquisição de direitos e como objeto de direito, merecendo tutela²²⁴. De acordo com o jusnaturalismo, para impulsionar um processo de laicização, o Direito deveria afastar-se da ideia de que os direitos provêm de forças divinas. O homem teria direitos, pois eles são próprios de sua natureza, trata-se da sua própria dignidade. Os jusnaturalistas defenderam essa concepção no século XVII. Um expoente dessa concepção foi Hugo Grócio²²⁵.

Contudo, os direitos de personalidade atingiram sua máxima dimensão no século XX, não por acaso. Afirmou Beck, em 1986, na apresentação de sua obra *Sociedade de risco*: “Pobre em catástrofes históricas este século na verdade não foi: duas guerras mundiais, Auschwitz,

²²³ VERBICARO, Dennis; CALANDRINI, Jorge. A proteção da confiança do consumidor e a base do legítimo interesse na Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). *Revista de Direito do Consumidor*, São Paulo, v. 31, n. 139, jan./fev. 2022, p. 91-92.

²²⁴ SARMENTO, Daniel. *Direitos fundamentais e relações privadas*. 2. ed., 3. tir. Rio de Janeiro: Lumen Juris, 2010, p. 122.

²²⁵ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 46.

Nagasaki, logo Harrisburg e Bhopal, e agora Chernobyl”²²⁶. Não há dúvida de que esses acontecimentos, em especial a Segunda Guerra Mundial, foram importantes para o desenvolvimento da tutela da personalidade pelo direito²²⁷. Diante desses acontecimentos, os direitos fundamentais passaram a ser o centro das constituições e legislações infraconstitucionais. Antes de todas essas problemáticas, os direitos fundamentais eram concebidos apenas como uma barreira contra excessos estatais²²⁸.

Esse entendimento é oriundo da denominada teoria subjetiva dos direitos fundamentais, que atribuía um caráter individualista a esses direitos básicos. Todavia, com o desenvolvimento da dimensão objetiva dos direitos fundamentais, as constituições cristalizam os valores mais importantes de uma comunidade política, são a base jurídica de uma coletividade; por isso, seus preceitos e garantias devem irradiar-se por todo o ordenamento jurídico. Desse modo, os direitos fundamentais passam de garantias apenas perante o Estado para garantias das relações jurídicas sociais, incidindo sobre o direito privado²²⁹.

A partir desse movimento, a ciência jurídica distancia-se de uma visão excessivamente patrimonialista e incorpora a despatrimonialização do direito civil, reposicionando o ser humano no centro dos ordenamentos jurídicos²³⁰.

É nesse contexto que se fala em personalização do Direito Privado. Assim, os direitos da personalidade representam formas de proteção da dignidade da pessoa humana nas relações jurídicas. Esses direitos são provenientes do resguardo da dignidade da pessoa humana, princípio tipificado no artigo 1.º, III, da Constituição Federal. Trata-se, portanto, do mínimo necessário de proteção. A doutrina entende que os direitos de personalidade têm caráter personalíssimo por serem indissociáveis da pessoa do seu titular; desse modo, só o titular poderá exercer esses direitos. Outras características que merecem destaque são a intransmissibilidade, a indisponibilidade e a imprescritibilidade. Portanto, os direitos de personalidade não podem

²²⁶ BECK, Ulrich. *Sociedade de risco: rumo a uma outra modernidade*. São Paulo: Editora 34, 2011 p. 7.

²²⁷ Nesse sentido, ver: MORAES, Maria Celina Bodin de. Danos à pessoa humana: uma leitura civil-constitucional dos danos morais. In: SARLET, Ingo Wolfgang (org.). *Constituição, direitos fundamentais e direito privado*. 2. ed. Porto Alegre: Livraria do Advogado, 2006, p. 66-67; SARMENTO, Daniel. *Direitos fundamentais e relações privadas*. 2. ed., 3. tir. Rio de Janeiro: Lumen Juris, 2010, p. 140.

²²⁸ “Os direitos fundamentais na Alemanha do pós-guerra, assim como no Brasil até a Constituição de 1988, só serviam para que o indivíduo se defendesse de uma eventual ingerência excessiva do Estado” (MORAES, *op. cit.*, p. 70).

²²⁹ Nesse sentido, ver: CANARIS, Claus-Wilhelm. *Direitos fundamentais e direito privado*. Tradução de Ingo Wolfgang Sarlet e Paulo Mota Pinto. Coimbra: Almedina, 2003; SARMENTO, Daniel. *Livres e iguais: estudos de Direito Constitucional*. Rio de Janeiro: Lumen Juris, 2006, p. 71-72: Sob esta ótica, “os direitos fundamentais protegem os bens jurídicos mais valiosos, e o dever do Estado não é só o de abster-se de ofendê-los, mas também o de promovê-los e salvaguardá-los das ameaças e ofensas provenientes de terceiros”.

²³⁰ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 49.

ser, em princípio, transferidos *inter vivos* ou *causa mortis*, nem são suscetíveis a alienação ou renúncia – podendo ser limitados em certas situações desde que com o consentimento do titular. Além disso, não se extinguem pelo não uso ou pela inércia na sua defesa, configurando-se como impenhoráveis e vitalícios²³¹.

Os direitos de personalidade devem ser uma cláusula geral, sua tutela é *numerus apertus* e não *numerus clausus*²³². Com efeito, “elege-se a concepção de que os direitos da personalidade seriam um complexo de interesses, voltados ao desenvolvimento da personalidade”²³³. Confirma esse entendimento em solo nacional o Enunciado n.º 274 do Conselho da Justiça Federal (CJF)²³⁴, que adotou a tese de Gustavo Tepedino, na IV Jornada de Direito Civil, em 2006. Para Tartuce, “existem outros direitos da personalidade tutelados no sistema, como aqueles constantes do Texto Maior. O rol do Código Civil é meramente exemplificativo (*numerus apertus*) e não taxativo (*numerus clausus*)”²³⁵.

Fala-se, portanto, em uma cláusula geral de tutela da pessoa, entendendo-se que os direitos de personalidade não podem ser tratados de forma estanque e “engessada”, sendo, então, por natureza versáteis e flexíveis, podendo ser adaptados conforme os anseios da sociedade²³⁶.

Tais direitos foram estipulados no Código Civil (CC) de 2002, estando tipificados nos artigos 11, 12, 16, 17, 20 e 21 do referido diploma legal. Ainda, o Diploma Civil estabelece, em seu artigo 2.º, que a “personalidade civil começa do nascimento com vida”, resguardado o direito do nascituro. Nessas disposições, são apontadas suas características: o direito ao nome, ao sobrenome e o direito de imagem. No caso de lesões, o legislador dispôs no artigo 21: “A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma”.

Com o desenvolvimento da doutrina de proteção de dados pessoais no mundo, essas informações passaram a ser consideradas extensões da personalidade dos indivíduos. O titular

²³¹ SARMENTO, Daniel. *Direitos fundamentais e relações privadas*. 2. ed., 3. tir. Rio de Janeiro: Lumen Juris, 2010, p. 122.

²³² ANDRADE, Fábio Siebeneichler de. A tutela dos direitos da personalidade no direito brasileiro em perspectiva atual. *Revista de Derecho Privado*, [s.l.], n. 24, p. 81-111, Enero-Junio 2013, p. 86. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/11474/2/A_Tutela_dos_Direitos_da_Personalidade_no_Direito_Brasileiro_em_Perspectiva_Atual.pdf. Acesso em: 22 jan. 2022.

²³³ *Ibid.*, p. 88.

²³⁴ A primeira parte da ementa do enunciado doutrinário prevê: “Os direitos da personalidade, regulados de maneira não exaustiva pelo Código Civil, são expressões da cláusula geral de tutela da pessoa humana, contida no art. 1.º, III, da Constituição (princípio da dignidade da pessoa humana). Em caso de colisão entre eles, como nenhum pode sobrelevar os demais, deve-se aplicar a técnica da ponderação” (TARTUCE, Flavio. *Manual de Direito Civil*. 11. ed., rev., atual. e ampl. Rio de Janeiro: Forense. 2021. *E-book*, cap. 2).

²³⁵ *Ibid.*, cap. 2.

²³⁶ BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor*. São Paulo: Almedina, 2019, p. 35.

dos dados não pode renunciar a seu direito sobre esses signos, além de ser sempre o titular daquelas informações, que não são passíveis de alienação.

Com o advento da sociedade da informação e, conseqüentemente, com a economia sendo orientada pelos dados, *os signos identificadores do cidadão* tornaram-se preciosos para as empresas. Assim, “cada vez mais, as atividades de processamento de dados têm ingerência na vida das pessoas”²³⁷. Dessa maneira, um dado atrelado à esfera de uma pessoa pode inserir-se nos direitos da personalidade, mas Bioni salienta que “ele deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular”²³⁸. Com efeito, justifica-se enquadrar, *dogmaticamente*, os dados pessoais na categoria dos direitos de personalidade²³⁹.

Logo, considerar os dados pessoais como unicamente relacionados com a privacidade implica restringir importantes reparações de danos que os usuários sofrem no ciberespaço, pois situações de discriminação algorítmica e o direito à retificação e de acesso aos dados não estariam abarcadas²⁴⁰.

Para a consolidação desse entendimento, foi essencial a decisão do Tribunal Constitucional alemão em 1983 – uma decisão paradigmática para a disciplina de proteção de dados. Nesse caso, passou-se a considerar os dados pessoais como extensões das personalidades dos indivíduos para além da lógica do público e do privado, compreendendo-se que a *finalidade* da coleta e do tratamento de dados é fundamental para orientar uma operação de dados, resguardando direitos dos titulares. Analisa-se a seguir essa decisão paradigmática antes de aprofundar o desenvolvimento das leis de proteção de dados pessoais, em especial a LGPD.

2.1.1.3 O direito à autodeterminação informativa

Em 1983, a Lei do Censo alemã determinou que os cidadãos fornecessem diversos dados para uma mensuração estatística, espacial e geográfica da população; entretanto, a sociedade civil sentiu-se ameaçada, o que provocou um impasse. A questão residia no fato de que esses dados coletados poderiam ser cruzados com outros registros públicos para a finalidade genérica

²³⁷ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 57.

²³⁸ BIONI, *loc. cit.*

²³⁹ BIONI, *loc. cit.*, grifo do autor.

²⁴⁰ *Ibid.*, p. 58.

de “atividades administrativas”²⁴¹. Em razão dessa incerteza, uma série de reclamações foi levada ao tribunal.

O Tribunal Constitucional alemão entendeu que a Lei do Censo era parcialmente inconstitucional. Bioni destaca a relevância do julgado pela sua *ratio decidendi*: a) a proteção de dados pessoais como direito de personalidade autônomo; b) a compreensão da autodeterminação informacional para além do consentimento e os limites dessa concessão, reiterando-se a importância do princípio da finalidade. O julgado é extremamente relevante por estabelecer que os cidadãos devem ter o controle das suas informações pessoais e por considerar tais dados como a extensão da personalidade dos indivíduos. Dessa forma, os dados pessoais não estariam apenas ligados ao direito à privacidade, mas estariam especialmente vinculados ao direito de personalidade. Assim, o uso de informações pessoais não deve afetar o livre desenvolvimento dos titulares²⁴².

Dada a importância do *controle* por parte dos cidadãos sobre suas informações pessoais, cunhou-se a expressão autodeterminação informativa²⁴³. Doneda lembra que esse ideal já era propagado por Westin em 1970. Com as tecnologias da informação, o aspecto informativo da privacidade assume uma nova dimensão, sendo fundamental para o desenvolvimento de um indivíduo na sociedade, permitindo, assim, a liberdade de opinião, de associação e de construção da sua intimidade²⁴⁴.

Além disso, Doneda reconhece o vanguardismo da decisão para a tutela da proteção de dados, pois já se destacavam as transformações tecnológicas, compreendendo-se que o direito à autodeterminação informativa é uma conjugação da personalidade da pessoa com sua participação social na comunidade²⁴⁵.

Como já explicitado, o ponto de partida do conceito de privacidade defendido por Warren e Brandeis tinha como figura central a ideia de sigilo, de espaço privado. Contudo, a evolução no conceito de privacidade levou ao foco *no controle*, isto é, à possibilidade de construção da esfera privada parcial ou total pelo titular das informações²⁴⁶. Por esse motivo,

²⁴¹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 97.

²⁴² *Ibid.*, p. 98-99.

²⁴³ *Ibid.*, p. 98.

²⁴⁴ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2021. *E-book*, cap. 2.

²⁴⁵ DONEDA, *loc. cit.*

²⁴⁶ “Uma definição da privacidade como ‘direito de ser deixado só’ perdeu há muito tempo seu valor genérico, ainda que continue a abranger um aspecto essencial do problema e possa (deva) ser aplicada a situações específicas. Na sociedade da informação tendem a prevalecer definições funcionais da privacidade que, de diversas formas, fazem referência à possibilidade de um sujeito conhecer, controlar, endereçar, interromper o fluxo das informações a ele relacionadas” (RODOTÁ, Stefano. *A vida na sociedade da vigilância: a privacidade*

Rodotà leciona: “Assim, a privacidade pode ser definida mais precisamente, em uma primeira aproximação, como o direito de manter o controle sobre as próprias informações”²⁴⁷.

Nesse sentido, a sentença do Tribunal Constitucional alemão é essencial para rejeitar a ideia de que certos dados são irrelevantes para a privacidade. De fato, as informações podem gerar riscos para os cidadãos dependendo de sua finalidade e de seu contexto. Desse modo, considerando o poder de armazenamento de dados das tecnologias da informação em diversos bancos, torna-se evidente a possibilidade de cruzamento desses dados teoricamente irrelevantes para identificar total ou parcialmente seu titular²⁴⁸.

Sobre esse direito fundamental, Doneda aponta algumas questões que o termo “autodeterminação” pode suscitar no intérprete. Em uma leitura liberal, o conceito de autodeterminação pode levar a pensar que esse direito se resume e concentra-se no ato do consentimento. Assim, se o titular consentiu com o tratamento de certos dados, ele exerceu sua autodeterminação porque escolheu. Todavia, não é necessário muito desenvolvimento argumentativo para notar que esse entendimento vai na contramão da *ratio decidendi* da decisão que cunhou o termo “autodeterminação informativa”. Além disso, tal entendimento faria que o consentimento tivesse um contorno negocial. Outra questão: os titulares têm direitos patrimoniais sobre os dados, o que é totalmente incompatível com a ideia de dados pessoais como direitos fundamentais dos cidadãos na sociedade tecnológica²⁴⁹.

Ao contrário de uma leitura liberal, defende-se que o direito de autodeterminação informativa, na realidade, retira o protagonismo do consentimento, colocando o princípio da finalidade como *a figura central* na proteção de dados. Sendo assim, elimina-se a total responsabilidade pelo controle de dados atribuída apenas ao titular; assume-se uma análise da finalidade e do contexto de coleta das informações, pois, como será desenvolvido em capítulo específico, os titulares enfrentam diversas dificuldades que desmistificam a ideia de controle das informações por meio do consentimento, sendo necessário criar instrumentos coletivos de controle de dados.

Nesse sentido, constata-se a importância do direito à autodeterminação informativa para a disciplina da proteção de dados pessoais pelo globo, não sendo por acaso que esse é um fundamento da Lei Geral de Proteção de Dados Pessoais, conforme o artigo 2.º, II. Além disso,

hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 92).

²⁴⁷ RODOTÀ, *loc. cit.*

²⁴⁸ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2021. *E-book*, cap. 2.

²⁴⁹ DONEDA, *loc. cit.*

ressalta-se que o entendimento de que a autodeterminação informativa é um instrumento de controle da coleta e do tratamento de dados é essencial neste trabalho. De fato, a autodeterminação informativa é entendida neste trabalho como o direito de controle das informações pessoais, a possibilidade de construção da esfera privada do titular a partir do princípio da finalidade e de uma análise contextual da coleta e do tratamento de dados.

Portanto, a proteção de dados pessoais é uma disciplina que deve ser concebida com base em seus fundamentos: privacidade, personalidade e autodeterminação informativa.

2.2 O DESENVOLVIMENTO DA MATÉRIA DE PROTEÇÃO DE DADOS

A criação de bancos de dados pelos Estados-Nações foi a mola propulsora para o desenvolvimento da matéria de proteção de dados. Nas décadas de 60 e 70 do século XX, diversos governos buscavam centralizar as informações dos cidadãos em gigantescos bancos de dados nacionais. Tal iniciativa ensejou uma reação dos cidadãos e da sociedade civil em razão das preocupações com o modo como essas informações seriam usadas pelos Estados²⁵⁰.

Para compreender a reação da sociedade contra os bancos de dados nacionais, é preciso lembrar que os Estados totalitários, como os nazifascistas, haviam sido derrotados há pouco menos de 20 anos, sendo uma lembrança e um temor recente nos pensamentos dos cidadãos que estavam entrando em Estados Democráticos de Direito. Para ilustrar essas preocupações a obra *1984*, de Orwell, traz um belo retrato das razões dos temores de um Grande Irmão na figura do Estado.

²⁵⁰ “Exemplo disso foi o caso do ‘National Data Center’, nos EUA, projeto que nunca saiu do papel naqueles moldes, dada a grande reação da população. De acordo com Simson Garfinkel, o ‘National Data Center’ foi proposto em 1965 pelo ‘Bureau of Budget’, órgão competente para administrar o orçamento, e visava à redução de custos pelo Estado. Sua ideia era a de que um único centro de dados nacional eximiria os demais órgãos do governo de investirem em informática e em tecnologia de armazenamento. No entanto, logo se percebeu que o centro traria inúmeras outras vantagens, tais como a possibilidade de se extraírem estatísticas de forma precisa e ágil, de se rastream e corrigirem inúmeros dados equivocados dos cidadãos e de utilizarem com grande eficiência os dados pessoais para as inúmeras atividades estatais, facilitando a tomada de decisões e o planejamento de ações. À medida que o projeto evoluiu, chegou-se à ideia de que o centro deveria conter dados de todos os cidadãos americanos em relação à data de nascimento, cidadania, registros escolares, serviço militar, registros de impostos, benefícios da previdência social, registro do espólio e, eventualmente, registros criminais. Procederam-se a inúmeras discussões nos meios de comunicação e a diversas audiências no Congresso. Esses debates culminaram em um senso comum acerca dos potenciais danos que tal centralização de dados poderia causar, principalmente em razão do grande poder que ele conferia ao Estado sobre a vida de todos os cidadãos, ameaçando gravemente a tradição liberal americana. Com essa repercussão, o ‘National Data Center’ nunca chegou a ser construído” (MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 29. Disponível em: <https://repositorio.unb.br/handle/10482/4782>. Acesso em: 11 abr. 2022).

Surge assim a denominada “primeira geração de leis de proteção de dados pessoais”. Das legislações pertencentes a essa geração, Doneda destaca a Lei do *Land* alemão de Hesse (1970), a legislação sueca que criou um Estatuto para os bancos de dados – *Datalag* (1973) – e a Lei de Privacidade estadunidense, de 1974²⁵¹.

Essas legislações tinham como objetivo regular o tratamento de dados, tendo como norte o cenário de grandes bancos de dados centralizados na figura do Estado. Para Bioni, essa geração de leis de proteção de dados é decorrente “das preocupações com o processamento massivo dos dados pessoais dos cidadãos na conjuntura da formação do Estado Moderno”²⁵². Segundo Doneda, não demorou para que esses regulamentos ficassem defasados em razão da constante evolução tecnológica e da descentralização dos bancos de dados²⁵³.

Laura Mendes concorda com Doneda: os dados pessoais antes centralizados primordialmente na figura do Estado descentralizaram-se, o que levou diversas organizações públicas e empresas privadas a ter amplo acesso a eles²⁵⁴. Em função da mudança gerada pela descentralização, inicia-se a chamada segunda geração de leis de proteção de dados pessoais.

Com a consciência da descentralização dos bancos de dados em diversos “pequenos irmãos”, a segunda geração de leis surgiu na metade da década de 70. Para Doneda, as legislações dessa geração focam a consideração da privacidade e a proteção dos dados pessoais como uma liberdade negativa, a ser exercitada pelo próprio cidadão²⁵⁵.

Observa-se que a estratégia regulatória do Estado para licenciar a criação e o funcionamento de todos os bancos de dados seria inviável. Desse modo, a segunda geração de leis transfere a responsabilidade para o próprio titular no que tange ao controle das suas informações pessoais. Cria-se assim um instrumento de controle por meio do qual o titular

²⁵¹ “Na década de 1970, surgiram as primeiras iniciativas legislativas para a tutela de dados pessoais. Entre as precursoras, a [...] Lei do *Land* alemão de Hesse, em 1970; a primeira lei nacional de proteção de dados que foi, na Suécia, o Estatuto para bancos de dados de 1973 – *Data Legen* 289, ou *Datalag* (que por sua vez também criava um inspetor para o uso de dados pessoais – o *Dataispektionen*), além do *Privacy Act* norte-americano em 1974. Estas iniciativas refletiam o estado da tecnologia e a visão da jurista à época, notadamente vinculada à experiência do *Data Center Nacional* e similares, marcada pela convicção de que direitos e liberdades fundamentais estariam ameaçados pela coleta ilimitada de dados pessoais, então realizada basicamente pelo Estado. Tais leis são hoje conhecidas como leis de ‘primeira geração’ de proteção de dados pessoais, em uma classificação por gerações que é um recurso usado habitualmente pela doutrina e do qual também lançamos mão, baseando-nos na classificação proposta por Mayer-Schönberger” (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2021. *E-book*, cap. 2).

²⁵² BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 110.

²⁵³ DONEDA, *op. cit.*, cap. 2.

²⁵⁴ MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *Revista dos Tribunais*, São Paulo, v. 108, n. 1009, caderno especial LGPD, nov. 2019, p. 39. Disponível em: https://www.academia.edu/42741177/A_lei_geral_de_prote%C3%A7%C3%A3o_de_dados_pessoais_um_modelo_de_tr%C3%AAs_n%C3%ADveis. Acesso em: 17 set. 2022.

²⁵⁵ DONEDA, *op. cit.*, cap. 2.

poderá optar por ceder suas informações ou não: o consentimento. Portanto, cabe exclusivamente ao titular controlar suas informações pessoais, o que suscita, como bem observa Laura Mendes, uma controvérsia sobre a efetividade do consentimento²⁵⁶.

Para Bioni, essa outorga de protagonismo ao titular é um divisor de águas para a terceira geração de leis sobre dados pessoais. Com efeito, a partir da terceira geração, busca-se assegurar que o indivíduo participará de todo o fluxo informacional das suas informações, desde a coleta até o compartilhamento. Nesse sentido, a decisão do Tribunal Constitucional alemão é um marco fundamental para esse entendimento ao sedimentar que o titular deve possuir o controle do fluxo das suas informações, determinando sua esfera privada²⁵⁷. Segundo Laura Mendes, a terceira geração distingue-se da segunda justamente por causa da participação do cidadão em todo o processo, que abarca o fluxo informacional na sua totalidade²⁵⁸. Contudo, Doneda adverte: o problema da terceira geração reside no fato de que poucos titulares estavam dispostos a exercer esse direito em razão dos custos sociais e econômicos²⁵⁹.

As leis de quarta geração pretendem sanar as deficiências das gerações anteriores, especialmente as da segunda geração. Percebeu-se que colocar a carga de responsabilidade apenas no titular não garante uma autodeterminação informativa, visto que há diversas desvantagens no controle individual²⁶⁰. Sendo assim, buscando satisfazer uma plena autodeterminação informativa, parte-se da premissa de que são necessários instrumentos

²⁵⁶ “A segunda geração de normas de proteção de dados pessoais suscita uma controvérsia bastante interessante, relacionada à efetividade do consentimento do cidadão e do real exercício de sua liberdade de escolha, em um contexto no qual a não disponibilização dos dados pode acarretar a sua exclusão social” (MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *Revista dos Tribunais*, São Paulo, v. 108, n. 1009, caderno especial LGPD, nov. 2019, p. 39. Disponível em: https://www.academia.edu/42741177/A_lei_geral_de_prote%C3%A7%C3%A3o_de_dados_pessoais_um_modelo_de_tr%C3%AAs_n%C3%ADveis . Acesso em: 17 set. 2022).

²⁵⁷ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 111.

²⁵⁸ “A principal diferença em relação segunda geração de normas é que a participação do cidadão no processamento de seus dados passa a ser compreendida como um envolvimento contínuo em todo o processo, desde a coleta, o armazenamento e a transmissão e não apenas como a opção entre ‘tudo ou nada’” (MENDES, *op. cit.*, p. 40).

²⁵⁹ “As leis de terceira geração encaravam a participação do cidadão como a mola propulsora de sua estrutura. Percebeu-se, no entanto, que não seriam muitas as pessoas dispostas a exercitar suas prerrogativas de autodeterminação informativa, dado que os custos envolvidos, fossem eles econômicos ou sociais, geralmente as compeliavam a aquiescer com situações que não eram as ideais. A autodeterminação informativa era, ainda, o privilégio de uma minoria que decidia enfrentar tais custos” (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2021. *E-book*, cap. 2).

²⁶⁰ “As leis de quarta geração, como as que existem hoje em vários países, caracterizam-se por procurar suprir as desvantagens do enfoque individual existente até então. Nelas, percebe-se uma consciência do problema integral da informação na fundamentação da disciplina, que implica na dificuldade de basear a tutela dos dados pessoais simplesmente na escolha individual – são necessários instrumentos que elevem o padrão coletivo de proteção. Nelas está presente igualmente uma dose forte de pragmatismo, voltado para a busca de resultados concretos” (DONEDA, *loc. cit.*).

coletivos de proteção de dados em conjunto com uma atuação qualificada de autoridades independentes²⁶¹, auxiliando o titular no exercício do seu direito.

Entende-se, por exemplo, que existem dados relativos a certos temas que são tão relevantes que não estão à disposição da esfera individual – como no caso dos dados considerados sensíveis. Verifica-se, dessa maneira, que a quarta geração retira o protagonismo apenas do titular, considerando outros fatores para além do ordinário consentimento.

Portanto, as legislações de quarta geração compreendem a vulnerabilidade do titular perante as novas tecnologias e os novos modelos de negócio das plataformas, procurando fortalecer os instrumentos de controle pelos titulares de maneira coletiva e preventiva. Como exemplo dessa quarta geração de leis, é possível citar a *General Data Protection (GDPR)* – regulamento europeu de 2016 – e a Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 2018 em solo nacional.

2.2.1 A Lei Geral de Proteção de Dados Pessoais (Lei n.º 13.709/2018)

As legislações sobre proteção de dados são fruto de anseios sociais globais, resultado de um movimento mundial que reivindica um maior controle dos dados pessoais em função da sua potencialidade para minar a personalidade dos cidadãos na sociedade tecnológica.

A LGPD é a primeira legislação geral no Brasil a tratar de forma específica do uso de dados pessoais. Contudo, é importante ressaltar que outras legislações setoriais abordavam o tema de maneira tangencial. O primeiro instrumento normativo brasileiro que abordava questões de dados pessoais é o *habeas data*, direito fundamental estabelecido no artigo 5.º, LXXII, da CF. Posteriormente, em 1990, o CDC regulou e autorizou o funcionamento dos bancos de dados no artigo 43, desde que respeitada a privacidade dos consumidores. O Código Civil, em 2002, também trata de proteção de dados pessoais, assim como a Lei do Cadastro Positivo (Lei n.º 12.414/2011), a Lei de Acesso à Informação Pública (Lei n.º 12.527/2011) e o Marco Civil da Internet (Lei n. 12.965/2014)²⁶².

Para a academia, a promulgação da LGPD era vital para uma regulamentação mais eficaz na proteção de dados pessoais, pois, como salienta Laura Mendes, “o tema era regulado

²⁶¹ BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020, p. 112.

²⁶² MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *Revista dos Tribunais*, São Paulo, v. 108, n. 1009, caderno especial LGPD, nov. 2019, p. 44. Disponível em: https://www.academia.edu/42741177/A_lei_geral_de_prote%C3%A7%C3%A3o_de_dados_pessoais_um_modelo_de_tr%C3%AAs_n%C3%ADveis. Acesso em: 17 set. 2022.

por diversas leis setoriais, formando uma verdadeira ‘colcha de retalhos normativa’²⁶³. Assim, a LGPD inicia um modelo *ex ante* de proteção de dados, compreendendo que não existem dados irrelevantes.

A legislação de dados brasileira caracteriza-se por ser um regulamento geral de matriz principiológica. Em relação ao seu aspecto principiológico, a escolha do legislador mostra-se adequada aos anseios de uma sociedade tecnológica. De fato, como bem ensina Claudia Lima Marques ao citar Erik Jayme, a pós-modernidade é um momento de extrema volatilidade e pluralidade, sendo necessário lançar um olhar diferenciado aos princípios que devem assumir o papel de bússola na aplicação das leis ante as rápidas mudanças características desse momento da história²⁶⁴.

2.2.1.1 Fundamentos e princípios

Os fundamentos da LGPD estão tipificados nos sete (7) incisos do artigo 2.º da Lei n.º 13.709/2018. Os setes fundamentos são:

- I - respeito à privacidade;
- II - a autodeterminação informativa;
- III - a liberdade de expressão, de informação, de comunicação e de opinião;
- IV - a inviolabilidade da intimidade, da honra e da imagem;
- V - o desenvolvimento econômico e tecnológico e a inovação;
- VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
- VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Conforme exposto ao longo deste trabalho, entende-se que a privacidade é um fundamento da LGPD por ser um elemento essencial para o desenvolvimento humano, precisamente para sua personalidade. Quanto à autodeterminação informativa, infere-se ser essencial a participação do titular em todo o fluxo informacional, controlando as informações e construindo sua esfera privada²⁶⁵.

²⁶³ “O tema era regulado por diversas leis setoriais, formando uma verdadeira ‘colcha de retalhos normativa’, o que suscitava inúmeras críticas, seja pela fragilidade da proteção do titular de dados pessoais, seja pela insegurança jurídica à qual se submetiam empresas que tinham como um dos pilares de seus negócios o tratamento de dados” (MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *Revista dos Tribunais*, São Paulo, v. 108, n. 1009, caderno especial LGPD, nov. 2019, p. 44. Disponível em: https://www.academia.edu/42741177/A_lei_geral_de_prote%C3%A7%C3%A3o_de_dados_pessoais_um_modelo_de_tr%C3%AAs_n%C3%ADveis . Acesso em: 17 set. 2022).

²⁶⁴ MARQUES, Claudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. São Paulo: Revista dos Tribunais, 2014, p. 191 *et seq.*

²⁶⁵ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais*. 3. ed. São Paulo: Revista dos Tribunais, 2019.

Em relação ao fundamento da liberdade de expressão, de informação, de comunicação e de opinião, Márcio Cots e Ricardo Oliveira aduzem que o legislador elegeu esses valores como um dos fundamentos da LGPD por serem direitos fundamentais presentes no texto constitucional e, principalmente, por proporcionarem o alicerce essencial ao desenvolvimento pessoal do indivíduo²⁶⁶. Para os autores, o fundamento da inviolabilidade da intimidade, da honra e da imagem é um desdobramento da proteção da privacidade, sendo natural sua tutela na legislação²⁶⁷.

O desenvolvimento econômico e tecnológico e a inovação buscam garantir o equilíbrio entre a tutela dos direitos dos usuários e o fomento da evolução tecnológica. Ressalta-se que o artigo 218 da Constituição estabelece que cabe ao Estado promover e incentivar o desenvolvimento científico. A legislação apenas ratifica que o Estado deve compatibilizar uma legislação protetora com o fomento da inovação, sem extremismos. Sobre o fundamento da livre-iniciativa, da livre-concorrência e da defesa do consumidor, a LGPD buscou, novamente, confirmar mandamentos constitucionais, corroborando o artigo 170 da CF, que trata da ordem econômica. Logo, a livre-iniciativa e a livre-concorrência devem estar em conformidade com a defesa do consumidor²⁶⁸.

Em relação aos últimos fundamentos – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais –, constata-se que há uma relação natural com os quatro primeiros fundamentos, visto que a privacidade, a autodeterminação informativa, as liberdades individuais e o respeito à personalidade *são direitos humanos dos titulares*. O legislador confirma esse entendimento ao tipificar no inciso VII, do artigo 2º da LGPD o direito “ao livre desenvolvimento da personalidade e à dignidade”.

Além de fundamentos bem definidos, que visam proteger o vulnerável nas relações assimétricas de coleta e de tratamento de dados, o legislador buscou princípios que possam guiar a aplicação das regulamentações sobre a proteção de dados. Os princípios demonstram-se fundamentais para as legislações que buscam regular as tecnologias da informação, pois as velocidades entre o Estado e as grandes companhias são diametralmente opostas. É vital que as leis não sejam extremamente específicas sobre certas tecnologias, sob pena de rápida defasagem. Nesse contexto, os princípios revelam-se extremamente importantes para enfrentar lacunas e problemáticas até então desconhecidas.

²⁶⁶ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais*. 3. ed. São Paulo: Revista dos Tribunais, 2019, p. 54.

²⁶⁷ *Ibid.*, p. 55.

²⁶⁸ *Ibid.*, p. 60.

Os princípios estão previstos no artigo 6.º da LGPD:

Art. 6.º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas²⁶⁹.

O princípio da finalidade, consagrado no artigo 6.º, I, da LGPD, tem o objetivo de delimitar o escopo final do tratamento dos dados pessoais, todo tratamento deve ser realizado com uma finalidade específica²⁷⁰. Com efeito, entende-se que o princípio da finalidade assume um papel central na análise do fluxo informacional a partir da decisão do Tribunal Constitucional alemão, sendo o grande norte para observar se o fluxo das informações respeitou as finalidades anteriormente solicitadas.

O princípio da adequação, tipificado no artigo 6.º, II, da LGPD, tem como foco evitar a desvirtuação da finalidade. Sendo a segunda fase de aferição após a análise da finalidade²⁷¹. A título de exemplo, se uma seguradora de saúde lida com dados sensíveis dos seus clientes, divulgando que serão utilizadas técnicas de anonimização para resguardar a proteção dos dados, mas realiza uma pseudoanonimização, aqui ocorrerá uma violação do princípio da

²⁶⁹ BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, edição 157, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 14 jan. 2022.

²⁷⁰ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais*. 3. ed. São Paulo: Revista dos Tribunais, 2019, p. 78.

²⁷¹ *Ibid*, p. 80.

adequação²⁷², visto que o procedimento do tratamento de dados como ofertado não foi adequado ao tratamento de dados sensíveis.

O princípio da necessidade, estabelecido no artigo 6.º, III, da LGPD, busca impedir o tratamento de dados excessivos ou desnecessários. Seu papel é analisar se um operador não está extrapolando a finalidade ao coletar demasiados dados. Esse princípio serve para compreender se a quantidade de dados coletados é realmente *necessária para se extrair a informação pretendida*. Portanto, questiona-se a forma de extração da informação que se pretende alcançar. Por exemplo, é necessário que um *streaming* saiba dados sensíveis de saúde para oferecer ao usuário uma sugestão de conteúdo? Não é possível realizar essa mesma “personalização” analisando outros tipos de dados?

Pode se dizer que o princípio do livre acesso, constante no artigo 6.º, IV, da LGPD, é uma extensão do remédio constitucional denominado *habeas data*, pois, enquanto esse direito fundamental refere-se às informações que estão em registros públicos ou de entidade de caráter público, o princípio ratifica e estende o livre acesso às informações agora na posse do mundo corporativo. Além disso, é um princípio que reforça o direito do consumidor à informação, previsto no artigo 6.º, III, do CDC. Garantem-se assim, as informações gratuitas ao titular, como o tempo de duração do tratamento de dados.

De acordo com o princípio da qualidade dos dados, disposto no artigo 6.º, V, da LGPD, as informações devem ser claras, exatas e relevantes para o tratamento que foi acordado entre o usuário e a plataforma.

O princípio da transparência, presente no artigo 6.º, VI, da LGPD, reforça a garantia aos titulares de informações claras, acessíveis e precisas, confirmando, mais uma vez, o direito básico à informação protegido pelo CDC.

O princípio da segurança (art. 6.º, VII, da LGPD) e o da prevenção (art. 6.º, VIII, da LGPD) impõem a utilização de técnicas e de medidas aptas para proteger os dados pessoais. São princípios que outorgam às plataformas a obrigação de utilizarem as técnicas mais evoluídas possíveis disponíveis no mercado para garantir a segurança e a prevenção, visando dirimir os riscos do tratamento de dados.

Pelo princípio da não discriminação, instituído no artigo 6.º, IX, da LGPD, dados pessoais, especialmente os sensíveis, não serão utilizados para constranger seus titulares. Desse modo, garante-se que os dados não sejam tratados para fins ilícitos e abusivos contra um dado indivíduo. Tal princípio revela-se um instrumento fundamental de tutela contra alguns

²⁷² COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais*. 3. ed. São Paulo: Revista dos Tribunais, 2019, p. 80.

problemas do comércio eletrônico, em que a oferta é governada por inteligência artificial –, que como já detalhado, pode produzir injustiças automatizadas, como, por exemplo, oferecer um produto apenas para uma nacionalidade.

Por último, mas não menos importante, o princípio da responsabilização e prestação de contas (art. 6.º, X, da LGPD), também denominado *accountability*, impõe aos agentes que demonstrem as medidas adotadas para garantir a segurança das informações dos usuários e o cumprimento das normas sobre o tema, sob pena de responderem civilmente pelos danos materiais e morais causados.

Sem retirar a importância dos princípios explicados, destacam-se o da finalidade (art. 6.º, I), o da adequação (art. 6.º, II), o da necessidade (art. 6.º, III), o da transparência (art. 6.º, VI) e o da responsabilização e prestação de contas (art. 6.º, X). Isso decorre da importância que esses princípios têm na análise de um fluxo informacional íntegro, respeitado o direito de autodeterminação informacional.

Os fundamentos são as raízes das disciplinas, suas bases fundantes. Compreender as estruturas de uma disciplina é essencial para a promoção de novos entendimentos que estejam de acordo com seus preceitos e objetivos. Logo, confirma-se, mais uma vez, que a proteção de dados só pode ser concebida com base no respeito dos direitos humanos, como a privacidade, a personalidade e as garantias individuais. Partindo desse pressuposto, os princípios são como um farol que guiará a aplicação da legislação, seja para compreender seu conteúdo axiológico, seja para preencher lacunas de aplicação que existirão em uma sociedade disruptiva.

Todos os fundamentos e princípios são instrumentos que garantem a aplicação e a proteção dos direitos dos titulares, resguardados no artigo 17 e seguintes da LGPD.

2.2.1.2 Os direitos dos titulares

A LGPD, em seu artigo 17, estipulou que “Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei”.

Inicialmente, verifica-se que o direito dos titulares se refere apenas às pessoas naturais, excluindo as pessoas jurídicas. Além disso, a LGPD, mais uma vez, reforça o respeito dos direitos fundamentais, demonstrando seu diálogo com os mandamentos constitucionais, como percebe-se na redação do artigo 17 do diploma.

O artigo 9.º da LGPD²⁷³ garante aos titulares o direito de acesso às informações sobre o tratamento de seus dados pessoais. É, portanto, um direito de a pessoa natural ter acesso facilitado às suas informações, dadas de forma clara, adequada e ostensiva. Dessa maneira, o titular tem o direito de saber a finalidade específica do tratamento (art. 9.º, I), ter acesso à informação sobre a forma e a duração do tratamento, desde que observados os segredos comercial e industrial (art. 9.º, II). O usuário tem ainda direito às informações de contato do controlador (art. 9.º, IV) e sobre o uso compartilhado de dados pelo controlador e a finalidade (art. 9.º, V). Igualmente no artigo 9.º, VI, da LGPD, garante-se ao titular a responsabilização dos agentes que realizarão o tratamento, estabelecendo-se uma *accountability* na LGPD. Ressalta-se que os parágrafos do artigo 9.º versam sobre importantes garantias relativas à validade do consentimento²⁷⁴.

Outro dispositivo da LGPD que consagra direitos dos titulares é o artigo 18, que dispõe: “O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição”. Nos nove (9) incisos do artigo²⁷⁵, há diversos direitos tipificados, como, por exemplo, o direito de confirmação da existência de tratamento (art. 18, I), a reiteração do direito de acesso (art. 18, II), o direito de correção de dados incompletos, inexatos ou desatualizados (art. 18, III), o direito de eliminação dos dados pessoais tratados com o consentimento do titular (art. 18, VI), com exceção das hipóteses do

²⁷³ “Art. 9.º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei”.

²⁷⁴ “§ 1.º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca. § 2.º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações. § 3.º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei”.

²⁷⁵ “Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; (Redação dada pela Lei n.º 13.853, de 2019) VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5.º do art. 8.º desta Lei”.

artigo 16²⁷⁶. Além dos mencionados, destacam-se os incisos VII, VIII e IX: o inciso VII trata do direito de informação sobre o compartilhamento de dados pelo controlador, com entidades públicas ou privadas; o VIII trata do direito de informação sobre a possibilidade de não fornecer consentimento e suas consequências negativas; o IX versa sobre a revogação do consentimento, nos termos do § 5.º do artigo 8.º da LGPD.

Os oito (8) parágrafos do dispositivo referem-se à instrumentalização dos direitos²⁷⁷, como o direito de peticionar contra o controlador perante a autoridade nacional (art. 18, § 1.º) e de opor-se ao tratamento realizado com fundamento em uma das hipóteses de dispensa do consentimento (art. 18, § 2.º).

2.2.1.3 O direito à proteção de dados pessoais como um direito fundamental

A reivindicação da proteção de dados pessoais como um direito fundamental é um debate antigo. Rodotà, por exemplo, defende essa consideração desde os anos 70. No Brasil, o debate reverbera há algumas décadas²⁷⁸.

Autores como Danilo Doneda e Laura Mendes defendem essa inserção no rol de direitos fundamentais desde o início do século XXI²⁷⁹. Nesse sentido, é importante ressaltar que, após

²⁷⁶ “Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados”.

²⁷⁷ “Art. 18 [...] § 1.º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional. § 2.º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei. § 3.º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento. § 4.º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3.º deste artigo, o controlador enviará ao titular resposta em que poderá: I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência. § 5.º O requerimento referido no § 3.º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento. § 6.º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional. (Redação dada pela Lei n.º 13.853, de 2019) Vigência § 7.º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador. § 8.º O direito a que se refere o § 1.º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor”.

²⁷⁸ RODOTÀ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 137 et seq.

²⁷⁹ DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2021. *E-book*; MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, DF, 2008, p. 14. Disponível em: <https://repositorio.unb.br/handle/10482/4782>. Acesso em: 11 abr. 2022.

anos de discussão doutrinária sobre considerar ou não o direito de proteção de dados pessoais como um direito fundamental, o Supremo Tribunal Federal (STF) terminou esse debate no ano de 2020.

Atualmente, não resta dúvida de que o direito de proteção de dados pessoais é um direito fundamental do cidadão brasileiro. Tal consagração ocorreu após a confirmação do STF no julgamento que suspendeu os efeitos da Medida Provisória (MP) n.º 954/2020. Lê-se na ementa da MP:

Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei n.º 13.979, de 6 de fevereiro de 2020.

A Fundação Instituto Brasileiro de Geografia e Estatística (IBGE) utilizaria os dados para alimentar a Pesquisa Nacional por Amostras de Domicílios (PNAD). Todavia, a MP foi objeto de diversas Ações Diretas De Inconstitucionalidade (ADI), como a ADI n.º 6.389, impetrada pelo Partido Socialista Brasileiro. As principais alegações para a inconstitucionalidade eram a falta de promoção dos direitos de personalidade e da autodeterminação informativa (art. 2.º, I e II, da Lei n.º 13.709/2018) e a não satisfação de requisitos importantes, como os princípios da LGPD, em especial, a finalidade (art. 6.º, I) e a adequação (art. 6.º, II).

Na decisão da ADI n.º 6.389, o STF ressaltou problemas na MP, dentre os quais merecem destaque:

- a) consideradas a necessidade, a adequação e a proporcionalidade da medida, não emerge da Medida Provisória n.º 954/2020, nos moldes em que foi editada, interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia;
- b) ao não definir apropriadamente como e para que serão utilizados os dados coletados, a MP n.º 954/2020 desatende a garantia do devido processo legal (art. 5.º, LIV, da CF), na dimensão substantiva, por não oferecer condições de avaliação de sua adequação e de sua necessidade, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades;
- c) ao não apresentar mecanismo técnico ou administrativo apto a proteger, contra acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a hígidez e, quando for o caso, o anonimato

dos dados pessoais compartilhados, a MP n.º 954/2020 descumpre as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros²⁸⁰.

Em seu voto, o Ministro Gilmar Mendes enumerou problemas relativos à questão formal, porque a MP trata de serviços de comunicação contrariando o disposto no artigo 21, XI, da CF; entretanto, o que mais merece destaque no voto do Ministro são as considerações sobre o direito fundamental à proteção de dados pessoais²⁸¹. Na sequência do seu voto, o Ministro defende o direito fundamental à proteção de dados pessoais na ordem constitucional brasileira²⁸².

O constitucionalista adverte: “a força normativa do direito fundamental à proteção de dados decorre da necessidade indissociável de proteção à dignidade da pessoa humana ante a contínua exposição dos indivíduos aos riscos de comprometimento da autodeterminação informacional nas sociedades contemporâneas”²⁸³.

A relatora da ADI, Ministra Rosa Weber, afirmou que, no contexto da sociedade da informação tecnológica, não há dados irrelevantes, inofensivos ao livre desenvolvimento do indivíduo; por isso, todos os dados devem ser protegidos na conjuntura da datificação das vidas²⁸⁴. Nesse mesmo sentido, o Ministro Fux alertou sobre a necessidade de proteger esse *commodity* da economia da informação e ressaltou a importância dessa salvaguarda em questões eleitorais²⁸⁵.

²⁸⁰ BRASIL. Supremo Tribunal Federal (Plenário). *Ação Direta de Inconstitucionalidade 6.389 DF 0090573-97.2020.1.00.0000*. Relatora: Min. Rosa Weber. Julgamento: 17 nov. 2020. Disponível em: <https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protECAo.pdf>. Acesso em: 27 set. 2022. p. 4 *et seq.*

²⁸¹ “Essa abrangência da proteção atribuída ao direito de autodeterminação constitui importante chave interpretativa do âmbito de proteção do direito fundamental à proteção de dados pessoais, o qual não recai propriamente sobre a dimensão privada ou não do dado, mas sim sobre os riscos atribuídos ao seu processamento por terceiros. Nesse aspecto, anoto brevemente que não merece prosperar o argumento de que o compartilhamento autorizado pela MP 954/2020 não envolveria dados sensíveis, já que o art. 2.º da norma autorizaria a transferência apenas da relação de ‘*nomes, números de telefone e endereços de seus consumidores, pessoas físicas ou jurídicas*’. É que, conforme será desenvolvido a seguir, no presente voto, a tutela de um direito fundamental à proteção de dados não mais se adstringe à demarcação de um espaço privado, mas, antes, afirma-se no direito à governança, transparência e sindicabilidade do tratamento de dados compreendidos em acepção abrangente” (*Ibid.*, p. 20, grifo do autor).

²⁸² “A afirmação da autonomia do direito fundamental à proteção de dados pessoais – há de se dizer – não se faz tributária de mero encantamento teórico, mas antes da necessidade inafastável de afirmação de direitos fundamentais nas sociedades democráticas contemporâneas. Considerando que os espaços digitais são controlados por agentes econômicos dotados de alta capacidade de coleta, armazenamento e processamento de dados pessoais, a intensificação do fluxo comunicacional na internet aumenta as possibilidades de violação de direitos de personalidade e de privacidade” (*Ibid.*, p. 21).

²⁸³ *Ibid.*, p. 22.

²⁸⁴ VICENTE, João Paulo. Decisão histórica do STF estabelece proteção de dados pessoais como direito fundamental. *Dadocracia by Data Privacy Brasil*, 30 mar. 2021. *Podcast* [5m 57s]. Disponível em: <https://dataprivacy.com.br/dadocracia-episodio-49-os-primeiros-processos-com-base-na-igpd/>. Acesso em: 23 ago. 2022.

²⁸⁵ *Ibid.*

No fim, o STF considerou a MP n.º 954/2020 inconstitucional por 10 votos a 1. Por conseguinte, a ação do governo federal não entrou em vigor.

Nota-se, portanto, que se trata de uma decisão paradigmática sobre a tutela dos dados pessoais, ultrapassando o entendimento dos dados voltados apenas para a tutela da privacidade. Compreendendo que os dados estão vinculados à personalidade das pessoas, não sendo importante a dicotomia público-privado.

Em razão desse entendimento, o Legislativo brasileiro decidiu emendar a Constituição Federal para estabelecer os dados pessoais como um direito fundamental, tornando a proteção de dados uma cláusula pétrea²⁸⁶. Tal disposição vai ao encontro do defendido pela doutrina nacional e internacional sobre o tema há décadas, reforçando o respeito à disciplina de proteção de dados pessoais no Brasil.

Sem dúvida, a constitucionalização da proteção de dados é uma grande salvaguarda para os usuários em solo brasileiro, garantindo ainda mais o respeito a esse direito fundamental nas relações privadas. Espera-se, também, que com essa nova dimensão da proteção de dados, os órgãos de fiscalização e de defesa dos consumidores atuem de maneira proativa e preventiva para garantir o respeito à privacidade e à intimidade dos usuários consumidores.

2.3 O DIREITO E A PROTEÇÃO DA CONFIANÇA DO INDIVÍDUO NAS RELAÇÕES CONTRATUAIS

Falar de confiança no Direito é uma tarefa desafiadora. Trata-se de um conceito transdisciplinar, diversas áreas do conhecimento buscaram ter esse tema como objeto de análise. Por exemplo, para a economia neoclássica, as pessoas deveriam confiar nas outras apenas se houvesse um interesse pessoal material; já para a psicologia, confiar é aceitar um estado de vulnerabilidade com base em expectativas positivas das intenções e do comportamento do outro²⁸⁷.

²⁸⁶ PROTEÇÃO de dados pessoais passa a ser direito fundamental. *CONJUR*, 10 fev. 2022. Disponível em: <https://www.conjur.com.br/2022-fev-10/protecao-dados-pessoais-passa-direito-constitucional>. Acesso em: 23 fev. 2022.

²⁸⁷ “According to neoclassical economics, people should trust others if and only if it is in their material self-interest to do so. Ultimately, this definition means that people should trust only when it is also in the self-interest of the person being trusted to respond in a mutually rewarding manner – such as when a trustworthiness is forced or when the failure of such a response is subject to punishment [...]. Such a definition of trust has a long philosophical tradition back to Socrates and Plato and can also be found in Machievelli’s *The prince* and Hobbes’ *Leviathan* [...]. However, from a psychological perspective and everyday experience, trust seems to be something more. People trust others even when there is no guarantee that the trustee will respond benevolently. Trust implies an awareness of being vulnerable to and dependent on the trustee – and still taking the risk of being exploited” (FETCHENHAUER, Detlef; DUNNING, David. Do people trust too much or too little? *Journal of*

Como salienta Manuel Carneiro da Frada, a confiança é objeto de investigação de diversos campos do conhecimento²⁸⁸. Segundo o autor português, para a ciência jurídica, confiança é um conceito incerto, não existindo uma definição legal da confiança. Contudo, é inegável que existe uma íntima relação entre confiança e direito, especialmente no que tange aos negócios jurídicos e contratos.

Diante da complexidade do tema, é necessário fazer uma análise transdisciplinar, examinando as concepções da sociologia e da psicologia sobre a confiança, pois, indubitavelmente, trata-se de um valor social, a mola da engrenagem que permite uma sociedade harmônica.

Considerando a importância da confiança para as relações negociais, é imperdoável que a ciência jurídica não aprofunde sua análise, sobretudo no que se refere às relações no ciberespaço, particularmente à concretização e ao desenvolvimento dos contratos ali firmados.

Como Mucelin explica, o contrato acompanha o que é consumidor²⁸⁹, estando suscetível a mudanças em razão de novas formas e de novos objetos de consumo. No mesmo sentido, para André Schmidt Neto, em uma sociedade complexa, nem os contratos ou leis conseguem acompanhar o desenvolver das relações humanas e suas profundidades²⁹⁰, sendo necessário um constante aprimoramento do direito para responder aos anseios e legítimas expectativas dos indivíduos.

Ante as mudanças no consumir, é papel do direito responder aos anseios dos cidadãos, nesse caso, consumidores digitais. Nesse sentido, Manuel Carneiro da Frada é lúcido ao apontar que “cabe a qualquer ordem jurídica a missão indeclinável de garantir a confiança dos sujeitos, porque ela constitui um pressuposto fundamental de qualquer coexistência ou cooperação pacífica, isto é, da paz jurídica”²⁹¹.

Economic Psychology, [s.l.], n. 30, 2009, p. 264. Disponível em: <https://sites.lsa.umich.edu/sasi/wp-content/uploads/sites/275/2015/11/fetchdunn.jep09.pdf>. Acesso em: 15 mar. 2022).

²⁸⁸ “Assim, ao corresponder a um fenómeno psíquico, ela [a confiança] constitui objecto natural da psicologia. A confiança interessa por outro lado também, e de sobremaneira, à sociologia jurídica, que encara como factor primordial da ordem social, simultaneamente causa e efeito de fenómenos jurídicos aí observáveis. Estes não constituem todavia o nosso ângulo de observação” (FRADA, Manuel A. Carneiro da. *Teoria da confiança e responsabilidade civil*. Lisboa: Almedina, 2015. Reimpressão da edição de fevereiro de 2004. p. 24-25).

²⁸⁹ MUCELIN, Guilherme. *Conexão online e hiperconfiança: os players da economia do compartilhamento e o direito do consumidor*. São Paulo: Revista dos Tribunais, 2020. *E-book*, cap. 3.

²⁹⁰ “Assim, em uma sociedade complexa, nem os contratos nem as leis acompanham o comportamento cultural e o significado dos símbolos que compõem a comunicação nos contatos sociais. O ato de confiar torna vulnerável aquele que crê verdadeiro algo que não está expresso nem no acordo, nem na lei, mas que é capaz de provocar uma expectativa legítima no contexto da contratação” (SCHMIDT NETO, André Perin. *Contratos na sociedade de consumo: vontade e confiança*. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*, cap. 3).

²⁹¹ FRADA, Manuel A. Carneiro da. *Teoria da confiança e responsabilidade civil*. Lisboa: Almedina, 2015. Reimpressão da edição de fevereiro de 2004. p. 19.

Portanto, para alcançar o que se pretende neste trabalho – demonstrar a necessidade de uma proteção de dados pessoais com base na valorização da confiança, estimulando deveres de informação, transparência e responsabilidade –, é fundamental considerar a confiança como um valor social para compreender a motivação da sua tutela pela ciência jurídica.

2.3.1 A confiança como um valor social

Na vida moderna, o ser humano, invariavelmente, é obrigado a confiar em pessoas que não conhece a fundo, assim como em instituições, empresas, métodos e sistemas. Pesquisas da área de economia comportamental demonstram que o ser humano é propenso a confiar ou a desconfiar dependendo de diversos fatores – a linha entre as duas tendências é bem tênue²⁹².

Pesquisas demonstram que os indivíduos julgam com base na familiaridade. Logo, tendemos mais a confiar em pessoas que se assemelham fisicamente àquelas com as quais convivemos. Por outro lado, o ser humano desconfia de quem tem características encontradas em pessoas conhecidas como desonestas. Para Chamorro-Premuzic, professor de psicologia em Columbia, isso leva os indivíduos a cometerem erros na hora de outorgar sua confiança²⁹³.

O erro é decorrente do falso julgamento que a premissa da familiaridade fornece ao indivíduo, fazendo com que o sujeito confie em alguém não aconselhável apenas a partir da familiaridade ou, por outro lado, desconfie de alguém confiável pelo mesmo critério.

Percebe-se que, pelo prisma da psicologia, confiar pode ser perigoso, pois confiar é aceitar riscos²⁹⁴. Não existem dúvidas de que os seres humanos são obrigados a confiar para viver em sociedade. É preciso, por exemplo, confiar nos avanços tecnológicos e em seus riscos desconhecidos. Portanto, a confiança é fluida e indispensável em qualquer relação social.

A confiança sempre foi um valor muito caro para a sociedade, assumindo um papel central nas relações humanas. O fator confiança nas relações sociais é objeto de estudo por vários autores, como Kant, Habermas e Luhmann, que buscaram demonstrar a importância desse valor para os sistemas sociais²⁹⁵. Além disso, na sociedade tecnológica, a confiança

²⁹² FETCHENHAUER, Detlef; DUNNING, David. Do people trust too much or too little? *Journal of Economic Psychology*, [s.l.], n. 30, 2009, p. 273 *et seq.* Disponível em: <https://sites.lsa.umich.edu/sasi/wp-content/uploads/sites/275/2015/11/fetchdunn.jep09.pdf>. Acesso em: 15 mar. 2022.

²⁹³ PIFFERO, Luiza. Confiança: por que é importante e porque pode te prejudicar. *GZH Comportamento*, 29 nov. 2019. Disponível em: <https://gauchazh.clicrbs.com.br/comportamento/noticia/2019/11/confianca-por-que-e-importante-e-por-que-pode-te-prejudicar-ck3k3o9mm00yy01rzgyvfmap6.html>. Acesso em: 15 out. 2022.

²⁹⁴ FETCHENHAUER; DUNNING, *op. cit.*, p. 273.

²⁹⁵ MARIÑEZ SÁNCHEZ, César David. La confianza: aproximaciones teóricas y propuesta sistémica para su abordaje en las ciencias sociales. *Século XXI: Revista de Ciências Sociais*, Santa Maria, RS, v. 2, n. 1, jan./jun. 2012, p. 175-179.

apresenta-se como um ativo sem igual, um valor social que possibilita a consolidação das relações negociais no ciberespaço.

Todos os dias os indivíduos são incentivados a realizar negociações. Contudo, em uma sociedade dinâmica, rápida e desmaterializada, os negócios sofrem mudanças marcantes, sendo cada vez mais impessoais e sem barreiras geográficas. Nesse cenário, a confiança apresenta-se como um *valor* fundamental. A confiança assume o papel de facilitadora para os contratantes, garantindo a fiabilidade entre as partes, gerando o *animus* de firmar uma negociação por acreditar que o seu objeto será cumprido e respeitado. Além de reduzir a complexidade de contratar, a confiança permite a prolongação da relação entre os sujeitos, tanto pessoal como comercial.

Não é difícil constatar a importância da confiança para as empresas, especialmente no comércio digital. Como bem analisa Claudia Lima Marques, como os consumidores precisam ter confiança no comércio eletrônico, é necessário proteger o vulnerável nas negociações realizadas pelo meio virtual, como, por exemplo, na ação de coleta de dados²⁹⁶.

O paradigma tecnológico impõe constantes atualizações dos produtos e serviços, que, por sua vez, carregam o risco da inovação. Desse modo, as empresas que contam com a confiança dos consumidores estão em um patamar mais avançado do que as concorrentes para estimular o consumo, pois, como ensina Celia Weingarten, a confiança permite a expansão das estratégias das empresas²⁹⁷.

O caso da Apple é emblemático para ilustrar os ensinamentos de Weingarten. A gigante tecnológica iniciou suas vendas no mercado consumidor com computadores pessoais em 1970. Nos anos 2000, lançou o *Ipod*, um aparelho de armazenamento de música portátil, e, em 2007, lançou o *Iphone*. Em seguida, lançou a *Apple tv* e o *Apple watch*. Observa-se, portanto, que, em razão da alta confiança do mercado consumidor na marca, a empresa expandiu seu negócio para vários tipos de bens tecnológicos diferentes, como celular, relógio e televisão.

Com tantas inovações de serviços e produtos em rápida velocidade, resta ao consumidor confiar. Por exemplo, o consumidor não tem alternativa a não ser acreditar que a coleta de dados por uma plataforma respeitará a finalidade requerida, assim como tem de acreditar que a

²⁹⁶ MARQUES, Claudia Lima. Proteção do consumidor no comércio eletrônico e a chamada nova crise do contrato: por um direito do consumidor aprofundado. *Revista de Direito do Consumidor*, São Paulo, v. 15, n. 57, jan./mar. 2006, p. 33 *et seq.*

²⁹⁷ “La confiabilidad de la marca y la empresa posibilita diseñar otro tipo de estrategias optimizando el beneficio económico; una empresa podrá por ejemplo ampliar y diversificar sus productos o servicios de manera mucho más sencilla, porque a través de la calidad de un producto el consumidor presumirá la calidad de otros (la expansión de la confiabilidad se representa en otros productos con la misma marca)” (WEINGARTEN, Celia. El valor económico de la confianza para empresas y consumidores. *Revista de Direito do Consumidor*, São Paulo, n. 33, jan./mar. 2000, p. 40).

inteligência artificial não o discriminará.

A relação entre comércio eletrônico e confiança é natural, fruto das características e da alta complexidade desse mercado. Como leciona de maneira magistral Claudia Lima Marques, nesse contexto tecnológico, é preciso um novo paradigma da confiança, entendida como uma redutora das complexidades no ciberespaço.

Os ensinamentos do sociólogo Niklas Luhmann são também essenciais para o desenvolvimento deste trabalho. Segundo Luhmann, além da confiança nas relações íntimas, *existe uma confiança nos sistemas sociais*. O sociólogo é um expoente da teoria de sistemas complexos; para ele, a sociedade é composta por diversos pequenos sistemas. Sendo assim, uma família é um sistema próprio, o Poder Judiciário é um sistema próprio, assim como o direito e assim por diante. Portanto, o que permite o funcionamento desses diversos sistemas em uma sociedade hipercomplexa sem o completo caos é a crença, a *fides*, a confiança nas pessoas e nas estruturas sociais²⁹⁸.

De acordo com Anthony Giddens, a confiança é decorrente da organização social moderna e dos sistemas peritos que estão em constante evolução²⁹⁹. Desse modo, a confiança é um valor de redução das complexidades no mundo moderno, é um valor que dirime riscos e confere segurança nas relações negociais e pessoais. Em serviços de alta especialidade, como os que são possíveis por meio da tecnologia e da *internet*, a comunidade não tem o saber técnico para entender na completude seu funcionamento e seus riscos. Como bem aponta Giddens, confiamos nos sistemas peritos, isto é, confiamos no sistema tecnológico composto por profissionais técnicos altamente especializados das *big techs*.

Para Luhmann, quanto mais complexo um sistema, mais confiança ele demanda, pois a confiança é uma redutora da complexidade, assim como um valor que legitima a operação daquele sistema. Portanto, para o sociólogo, sem confiança, não há um sistema em harmonia³⁰⁰.

Como adverte Luhmann, sem confiança, o homem nem sairia da cama, ficaria com um medo paralisante de que qualquer ação ou atitude resultaria em um desastre³⁰¹. Realmente, como explica Milhomens, a sociedade tecnológica impõe-nos relacionamentos fluidos, com pessoas estranhas ou máquinas que lidam com questões complexas da vida do cidadão. É

²⁹⁸ RODRIGUES, Léo Peixoto; NEVES, Fabrício Monteiro. *A sociologia de Niklas Luhmann*. Petrópolis, RJ: Vozes, 2017, p. 27 *et seq.*

²⁹⁹ GIDDENS, Anthony. *As consequências da modernidade*. Tradução de Raul Fiker. São Paulo: Unesp, 1991, p. 95.

³⁰⁰ “Donde hay confianza hay aumento de posibilidades para la experiencia y la acción, hay un aumento de la complejidad del sistema social y también del número de posibilidades que pueden reconciliarse con su estructura, porque la confianza constituye una forma más efectiva de reducción de la complejidad” (LUHMANN, Niklas. *Confianza*. Barcelona: Anthropolos, 1996, p. 103).

³⁰¹ *Ibid.*, p. 5.

impossível conhecer a fundo as pessoas com quem nos relacionamos nas negociações cotidianas³⁰², como na relação impessoal entre o consumidor e o motorista de aplicativo.

Nesse contexto, é a confiança que possibilita uma sociedade funcional, garantindo a estabilização das relações sociais e uma espécie de aceitação tácita dos sistemas peritos³⁰³. Além disso, Luhmann observa que uma das virtudes da confiança é a possibilidade de, ao menos em parte, assegurar o futuro, isto é, *garantir uma previsibilidade das ações* de uma empresa ou de um indivíduo, normalmente, analisando suas atitudes progressas³⁰⁴.

O ser humano passa a confiar em alguém ou em um sistema com o prolongamento da relação, pois, com o decurso do tempo, é possível analisar as ações do passado. Há, também, a confiança no conhecimento técnico-científico, nas instituições, como, por exemplo, de regulação³⁰⁵. Com efeito, em uma sociedade tecnológica, com a utilização maciça de máquinas, o cidadão está cada vez mais vulnerável, porque quem confia coloca-se em uma posição de risco.

2.3.2 A confiança e o direito privado

³⁰² “Sem conhecer a fiabilidade, valores e vida progressa das pessoas com as quais nos relacionamos, somos levados a pressupor a boa-fé e depositar confiança de que estes estranhos estão bem-intencionados em cumprir com sua parte nos acordos sociais celebrados. Se este estranho tiver um aporte de expertise garantido por um sistema abstrato, um tanto melhor. É nisso o fortalecimento da sociedade em rede ou de comunicação, através de ferramentas que possam reduzir as complexidades, detêm papel fundamental, onde as plataformas de consumo da economia do compartilhamento têm potencial para um importante contributo. Alternativa contrária, a total e irrestrita desconfiança nos levaria à beira da paranoia coletiva e inviabilizaria a própria vida em sociedade nos grandes centros urbanos” (MILHOMENS, Heitor Antunes. *Tutela da confiança e da vulnerabilidade na economia do compartilhamento: empoderamento do consumidor digital e mitigação da vulnerabilidade estrutural na era do hiperconsumo*. 2021. 228 f. Dissertação (Mestrado em Direito) – Universidade Federal do Pará, Belém, 2021, p. 103).

³⁰³ “A confiança, então, torna-se a aceitação tácita de circunstâncias nas quais outras alternativas estão descartadas. É a resignação de que, tanto quanto não podemos dominar todos os conhecimentos – e somos, assim, tecnicamente vulneráveis –, não podemos renunciar por completo aos complexos sistemas peritos em que estamos enredados pois não temos como deixar de consumir” (*Ibid.*, p. 107).

³⁰⁴ LUHMANN, *op. cit.*, p. 39 *et seq.*

³⁰⁵ “Pragmaticamente a confiança se reforça nas experiências anteriores, onde tais sistemas abstratos funcionaram da forma que se esperava. Há confiança, ainda, no conhecimento técnico-científico organizado no entorno do discurso do método e das associações profissionais, na força reguladora estatal que em alguma medida mantém vigilância sobre os padrões empregados pelos fabricantes e, mais recentemente, no debate público proporcionado pelos sistemas de reputação e avaliação próprios do capitalismo de plataforma. Ao passo que as relações sociais na hipermodernidade se tornaram hipercomplexas, não temos mais como deixar de confiar nos sistemas peritos como ferramentas de redução da complexidade, pelo que nos tornamos vulneráveis e hipossuficientes” (MILHOMENS, *op. cit.*, p. 108).

Carneiro da Frada salienta que a confiança é um tema de destaque no universo anglo-saxônico, citando obras de Lon Fuller e William Perdue³⁰⁶. Para o professor do Porto, a confiança não recebeu em outros países o aprofundamento que conheceu na Alemanha, país em que o tema recebeu mais atenção. A doutrina da confiança foi aprofundada de fato pelos juristas germânicos. A confiança foi estudada, inicialmente, sob o prisma da teoria da aparência, já no início do século XX. Contudo, Frada lembra que a matéria atingiu seu ápice com Claus-Wilhelm Canaris, discípulo do ilustre jurista Karl Larenz³⁰⁷.

Para Larenz, a confiança é um princípio imanente de todo o direito, que atua como diretriz das relações contratuais, agindo como um princípio “motor” da atuação do indivíduo, possuindo ligação direta com o princípio da responsabilidade. Segundo o jurista alemão, o princípio da confiança tem suas raízes no personalismo ético. Assim, a pessoa livre, social e racional determinará a si mesma³⁰⁸.

Canaris é o catedrático que aprofundou a responsabilidade pela confiança no direito privado, buscando sistematizar um direito ao ressarcimento de danos em razão de frustrações das expectativas legítimas. Cabe ainda lembrar que a confiança importa no debate dos negócios jurídicos, protegendo o confiante em suas legítimas expectativas no negócio³⁰⁹, assunto que será profundado.

Manuel Carneiro da Frada é uma referência no assunto em língua portuguesa. Em sua tese de doutorado, realizou uma profunda análise jurídica e dogmática da teoria da confiança voltada para o tema da responsabilidade civil a partir dos estudos da doutrina germânica sobre o tema. O autor salienta que a confiança é um objeto de estudo de diferentes áreas do Direito, como o campo da responsabilidade civil, do negócio jurídico e até da Filosofia do Direito, pois existe uma relação entre ética e confiança³¹⁰.

³⁰⁶ “Ela [a confiança] representa também designadamente um tema de destaque no universo anglo-saxónico. Esta realidade confirma o carácter fundamental de que a protecção da confiança se reveste no Direito, independentemente da singularidade e variabilidade dos direitos positivos” (FRADA, Manuel A. Carneiro da. *Teoria da confiança e responsabilidade civil*. Lisboa: Almedina, 2015. Reimpressão da edição de fevereiro de 2004. p. 37).

³⁰⁷ *Ibid.*, p. 35.

³⁰⁸ MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p. 185-186.

³⁰⁹ “A defesa da confiança está longe de se esgotar na atribuição de um direito ao ressarcimento de danos, operando, na realidade, de diferentes modos. Ela consente uma destrição fundamental, segundo as consequências a que pode dar lugar. Nalguns casos, a ordem jurídica preserva ou realiza a posição do confiante, por exemplo atribuindo à situação de confiança ocorrida os efeitos jurídicos equivalentes ao objecto da representação, como se ele tivesse realmente ocorrido” (MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p. 41).

³¹⁰ FRADA, Manuel A. Carneiro da. *Teoria da confiança e responsabilidade civil*. Lisboa: Almedina, 2015. Reimpressão da edição de fevereiro de 2004. p. 24-26.

É no ramo do direito privado que houve o desenvolvimento da teoria da confiança, estudando-se, por exemplo, as frustrações de expectativas, que podem desencadear pretensões indenizatórias. A teoria da confiança relaciona-se com os negócios jurídicos, desde a verificação da validade dos acordos até o cumprimento forçado das obrigações principais e conexas de conduta.

Nota-se a fertilidade do tema com seus múltiplos ângulos de investigação. Neste estudo, pretende-se aprofundar a análise do tema na perspectiva dos negócios jurídicos, especialmente considerando os deveres e as obrigações das partes contratantes, notadamente dos *players* na proteção de dados dos consumidores no ciberespaço. Abordar-se-ão ainda as pretensões indenizatórias em razão de expectativas de proteção de dados frustradas pelas plataformas.

2.3.2.1 As dimensões negativa e positiva da confiança

Existem uma proteção positiva e uma proteção negativa da confiança. Sobre as dimensões, Carneiro da Frada leciona: “Se a primeira se preocupa em assegurar ao sujeito ‘positivamente’ a sua expectativa, esta última ‘nega’ ao confiante o direito a ser colocado nessa situação, reconhecendo-lhe em vez disso um direito indenizatório (contra outrem)”³¹¹.

Andreza Baggio, em sua análise da confiança no direito privado, também salienta essas dimensões. O aspecto positivo da confiança constitui uma força vinculante do contrato, impondo o cumprimento de deveres anexos de conduta e o respeito das legítimas expectativas dos contratantes. Assim, privilegiam-se a segurança jurídica e a função social do contrato. A dimensão negativa atua como um critério de legitimidade do contrato, sendo um requisito daquele negócio jurídico, aferindo se não há abuso de direito de alguma das partes contratantes. No caso de haver abuso de direito e legítimas expectativas frustradas, a parte confiante poderá requerer uma indenização³¹².

Para Frada, a proteção positiva das expectativas preserva a posição do confiante, protegendo a crença do sujeito e suas consequências como se fosse uma situação jurídica real, assegurando positivamente sua legítima confiança³¹³. A negativa é a responsabilidade pela

³¹¹ MARQUES, *loc. cit.*, p. 42.

³¹² BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 100.

³¹³ FRADA, Manuel A. Carneiro da. *Teoria da confiança e responsabilidade civil*. Lisboa: Almedina, 2015. Reimpressão da edição de fevereiro de 2004. p. 41-42.

confiança em razão de frustrações de expectativas, contudo, salienta o autor, não se trata de uma confiança desvairada, trata-se de condutas objetivas³¹⁴.

Judith Martins-Costa explica que a dimensão negativa atua como um limite ao exercício de direitos. Assim, quando legítimas expectativas forem violadas, o confiante fará jus a uma indenização. A dimensão positiva, por sua vez, relaciona-se com a produção de efeitos de deveres jurídicos de condutas³¹⁵. Frada salienta que a tutela da confiança não deve ser reduzida ao simples ressarcimento indenizatório, pois sua defesa pode dar-se por outros meios, como, por exemplo, pela adequação do serviço à necessidade do consumidor, atuando de maneira positiva³¹⁶.

Lúcido, Frada toca em um ponto que é muito importante para o atual contexto tecnológico: em razão da dependência dos consumidores dos serviços tecnológicos, por vezes, é mais importante a continuidade da prestação contratual conforme as expectativas do usuário de que o desfazimento da relação com uma quantia indenizatória.

Portanto, o aspecto negativo da proteção da confiança transparece quando esse valor atua como um requisito de legitimidade das relações de consumo, por exemplo, aferindo a possibilidade de legítimas expectativas frustradas. Em relação ao aspecto positivo, a confiança assume o papel de fundamento para forçar o cumprimento da obrigação assumida entre as partes, aferindo a validade do contrato³¹⁷.

O fundamento da dimensão positiva da confiança é, nas palavras de Canaris, “um imperativo ético-jurídico”, ligado à boa-fé e à segurança jurídica³¹⁸. Para Canaris, a ordem jurídica não pode deixar de conferir relevância às expectativas do indivíduo confiante, pois é necessário proteger o tráfego jurídico. Aqui se enquadram a proteção do *venire contra factum*

³¹⁴ “No âmbito da proteção negativa das expectativas, a expressão ‘responsabilidade pela confiança’ não significa deste modo, meramente que alguém é chamado a suportar as consequências jurídicas da confiança alheia. Aquela locução tem também um conteúdo mais restrito: assinala o surgimento de um dever jurídico preciso, o de ressarcir um prejuízo” (*Ibid.*, p. 42).

³¹⁵ MARTINS-COSTA, Judith. Princípio da confiança legítima e princípio da boa-fé objetiva. Termo de Compromisso de Cessação (TCC) ajustado ao Cade. Critérios da interpretação contratual: os “sistemas de referência extracontratuais” (“circunstâncias do caso”) e sua função no quadro semântico da conduta devida. Princípio da unidade ou coerência hermenêutica e “usos do tráfego”. Adimplemento Contratual. *Revista dos Tribunais*, São Paulo, v. 95, n. 852, p. 87-126, out. 2006.

³¹⁶ “Ora, o escopo da proteção positiva da confiança – colocar o sujeito na situação correspondente à confiança que teve – pode ser alcançado por outros meios que não através da imposição de um sucedâneo indenizatório dessa situação; desde logo, por exemplo, pela cominação de um dever de conduta dirigido à satisfação ‘em espécie’ das expectativas alheias” (FRADA, *op. cit.*, p. 43).

³¹⁷ BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 126.

³¹⁸ MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p.185

proprium e certos vícios nos negócios jurídicos, devendo ser protegidas as legítimas expectativas da parte confiante³¹⁹.

Frada atribui à dimensão positiva a característica de ser aberta, sendo impossível circunscrever definitivamente situações abrangidas por essa tutela jurídica; logo, essa dimensão caracteriza-se por ser um sistema móvel³²⁰. Tal afirmação vai ao encontro do objetivo desse estudo, que busca defender a proteção positiva da confiança para assegurar a proteção das legítimas expectativas de proteção de dados, ampliando ainda mais o campo de atuação da dimensão positiva no Direito, agora voltada para garantir deveres de condutas anexos e principais nas relações de tratamento de dados. A partir da fundação de uma ética jurídica, os *players* devem atentar para as expectativas de proteção de dados dos usuários.

Examinadas as dimensões de proteção da confiança, importa demonstrar a evolução da teoria da confiança nos campos dos negócios jurídicos e da responsabilidade civil.

2.3.2.2 O desenvolvimento da teoria da confiança pelos estudos do negócio jurídico e a tutela da aparência

A responsabilidade pela aparência jurídica está no campo da proteção da confiança. A tutela da aparência busca, segundo Frada, “colocar o confiante na posição jurídica correspondente às expectativas que alimentou; a ordem jurídica confere a alguém uma posição que ‘em si’ não existia”³²¹. O autor elucida que a tutela da aparência “anula” a diferença entre o que parece e aquilo que realmente condiz com a realidade jurídica. Esclarece: “Esta corresponde a um *Tatbestand* de confiança especialmente intenso, pela enérgica tutela de expectativas que a ordem jurídica a ele associa”³²².

³¹⁹ “Manifestam este tipo de proteção da confiança o *venire contra factum proprium*, a *supressio* e a *surrectio*, certas situações de inalegabilidade de vícios de forma ou de outros vícios do negócio jurídico, hipóteses em que a errada interpretação de um negócio jurídico gerou expectativas, vindo uma das partes a querer prevalecer-se mais tarde do seu autêntico sentido, casos em que quem confiou na realização voluntária de uma prestação em si não imposta juridicamente vem a ser surpreendido pela recusa do seu cumprimento, etc.” (FRADA, Manuel A. Carneiro da. *Teoria da confiança e responsabilidade civil*. Lisboa: Almedina, 2015. Reimpressão da edição de fevereiro de 2004. p. 62-63).

³²⁰ “Em todo o caso, o facto de na génese deste tipo de proteção da confiança se encontrarem exigências indeclináveis postas por um princípio jurídico fundamental comunica-lhe um carácter aberto. É impossível proceder à circunscrição definitiva das situações abrangidas pela tutela jurídica, assim como não se apresenta viável organizar de modo rígido os elementos de que esta depende. Com razão se preconiza, quanto a esta modalidade de responsabilidade pela confiança, um sistema móvel, capaz de possibilitar uma concretização-aplicação flexível em função do caso” (*Ibid.*, p. 64).

³²¹ FRADA, Manuel A. Carneiro da. *Teoria da confiança e responsabilidade civil*. Lisboa: Almedina, 2015. Reimpressão da edição de fevereiro de 2004. p. 45.

³²² *Ibid.*

Verifica-se que a tutela da aparência está no âmbito da tutela positiva da confiança³²³, possuindo como fundamentos a proteção do tráfego e da segurança jurídica. Segundo Menezes de Cordeiro, a tutela da confiança premia a circulação de bens³²⁴ e, agora sem dúvida, de serviços.

A proteção do tráfego jurídico é cristalina na tutela da aparência, pois busca-se estabilizar relações jurídicas, privilegiando-se a posição do confiante e a circulação de bens e serviços. Mas as situações de aparência, adverte Frada, devem estar em previsões legais, dependentes da vontade do legislador, diferentemente de uma responsabilidade pela confiança³²⁵. Portanto, elas não se confundem.

Nos negócios jurídicos, a confiança apresenta a sua dupla dimensão: protege as expectativas dos negociantes, garantindo o cumprimento de deveres obrigacionais, principais ou anexos, e assegura um direito de ressarcimento, atuando positivamente e negativamente.

No Brasil, o ilustre e lendário Pontes de Miranda foi um dos grandes percursores dos estudos dos negócios jurídicos e da tutela da aparência, difundido as teorias em solo nacional. Pontes de Miranda notabilizou-se, entre outras coisas, pela sistematização do negócio jurídico em três planos: existência, validade e eficácia, identificando as diferenças entre eles. Mas, acima disso, o autor entende a vontade como um elemento privilegiado, pois compreende o *animus* como o elemento responsável pela formação e pela existência do contrato³²⁶.

Constata-se, por exemplo, que o Código Civil vigente absorveu ensinamentos de Pontes de Miranda no seu artigo 104³²⁷, que reconhece o plano da existência e da validade. É necessário que haja um agente capaz e que o objeto do negócio seja válido, ou seja, lícito, possível,

³²³ “No seu âmbito versam-se figuras como a procuração aparente, o casamento putativo, a proteção de terceiros em face da simulação, o preenchimento abusivo de declarações em branco, sociedades aparentes, a publicidade registal, a preclusão de meios de defesa em títulos de crédito, etc.” (*Ibid.*, p. 46).

³²⁴ “[...] equivale, no fundo, a premiar a circulação de bens, em detrimento da sua conservação estática” (CORDEIRO, António Menezes. *Da boa fé no direito civil*. Lisboa: Almedina, 2017, p. 1247).

³²⁵ “O propósito de dilucidar o efectivo alcance e cabimento de uma dogmática da confiança como fonte de responsabilidade civil não reclama contudo que nos detenhamos nesses meandros. Embora haja conexões com a tutela indemnizatória da confiança. O facto de as situações de proteção da aparência dependerem, em princípio, ao contrário desta, de previsões legais específicas que manifestam uma vontade explícita do legislador – a traduzir uma relativa fixação dos *tatbestand* envolvidos – não prejudica que a sua própria linha de fronteira em relação aos outros sectores da tutela da confiança, sobretudo ‘positiva’ como a que a seguir consideraremos, se apresente por vezes esbatida” (FRADA, *loc. cit.*, p. 51).

³²⁶ “A essa divisão estrutural do negócio jurídico apresentada pelo autor deu-se o nome de ‘escala ponteana’, na qual a vontade encontra-se privilegiada, pois é responsável pela existência do contrato. Para o mesmo autor são a vontade, o agente e o objeto que delimitam o surgimento do negócio jurídico, e, para que seja válido, será necessária a análise das qualidades destes elementos de existência ou seja, se o agente é capaz, o objeto é lícito e se a vontade foi manifestada dentro dos pressupostos legais” (BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 115).

³²⁷ “Art. 104. A validade do negócio jurídico requer: I - agente capaz; II - objeto lícito, possível, determinado ou determinável; III - forma prescrita ou não defesa em lei” (BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 11 jan. 2002. PL 634/1975. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 15 mar. 2022).

determinado ou indeterminado, mas nunca impossível. Entende-se, portanto, o negócio jurídico como todo fato jurídico decorrente de uma manifestação de vontade. A diferença entre fato e negócio jurídico está justamente na vontade do agente³²⁸.

No conceito do instituto do Código Civil, já é possível notar a importância da *vontade* – ponto que suscita grande controvérsia. Andreza Baggio, em sua obra *O direito do consumidor brasileiro e a teoria da confiança*, explica a construção da teoria da confiança nos estudos sobre o negócio jurídico. A professora rememora as teorias da vontade e da declaração sobre os negócios jurídicos, objeto de um debate importante no século XIX. Nessa época, reinava o dogma da autonomia da vontade, fruto do pensamento liberal que compreendia a vontade como a maior força vinculante de um negócio. Para Savigny, a vontade da parte é essencial no contrato, pois parte-se do pressuposto de que o homem é dotado de autonomia, assim, a vontade torna-se a força vinculante do negócio jurídico ou contrato, isto é, *pacta sunt servanda*³²⁹.

Nessa esteira, defende-se que o negócio não produzirá efeitos caso ocorra alguma divergência entre a vontade interna e a declarada. Quando, por exemplo, um negociante incide em erro, o negócio estará nulo. Contudo, nota-se muita abstração, pois como realmente defender qual seria a vontade interna de um sujeito? Como comprovar?

A aceitação da teoria era o resultado do entendimento segundo o qual “A vontade merecia proteção porque sua manifestação resultava da liberdade dos sujeitos, e somente tutelada a vontade, existiria segurança jurídica”³³⁰. À luz da teoria da vontade, o contrato era considerado um ato de autonomia privada. Se o negócio fosse insustentável, com cláusulas abusivas, deveria ser cumprido de qualquer maneira, pois a autonomia deveria ser respeitada.

Entretanto, o pensamento contratualista evoluiu ao perceber diversas desigualdades fáticas e materiais entre os negociantes ou contratantes, o que fez o Direito rever o dogma da vontade. Assim, em razão das críticas à teoria da vontade, inicia-se o desenvolvimento da teoria da declaração pelo direito germânico³³¹.

Para André Schmidt Neto, a constitucionalização do direito privado foi um grande passo para a superação da ótica voluntarista³³². Nesse sentido, busca-se analisar a vontade real e a

³²⁸ “Esta definição de negócio jurídico, ou seja, levando em conta a existência de uma manifestação de vontade determinante para a sua caracterização, é inclusive aceita no Brasil, e difundida pela maior parte dos doutrinadores. Observa-se que a distinção entre fato jurídico e negócio jurídico está justamente, neste último, de existência de atuação da vontade” (BAGGIO, *loc. cit.*, p. 114).

³²⁹ *Ibid.*, p. 89.

³³⁰ *Ibid.*, p. 90.

³³¹ *Ibid.*, p. 90-91.

³³² “A constitucionalização do Direito Privado foi o passo mais importante para a superação da ótica voluntarista. Em outras palavras, o direito privado sofre uma influência direta da Constituição, da nova ordem pública por ela imposta, e muitas relações particulares, antes deixadas ao arbítrio da vontade das partes, obtêm uma relevância jurídica nova e um conseqüente controle estatal, que já foi chamado de 'publicização do direito privado'”

declarada, aferindo se não há conflitos na decisão formalizada ou até tipos de vícios de vontade, como dolo, de consentimento, erro, coação e outros. Para Baggio, “Esta teoria tinha por fundamento o sentido formal da declaração de vontade, buscando-se tutelar a segurança e a estabilidade nas relações jurídicas, valorando-se a vontade declarada e não a intenção do sujeito”³³³.

A teoria da declaração volta-se para a análise da palavra dada, isto é, para a declaração do sujeito, enquanto o viés subjetivo da teoria da vontade foca as representações abstratas do declarante. Desse modo, a teoria busca adjetivar a declaração de vontade do agente, analisando se foi válida, sem coações ou erros, por exemplo. Assim, a meta é analisar a declaração no seu sentido formal, valorando-se a vontade declarada do sujeito e seu contexto.

Como um meio-termo entre a teoria da vontade e a teoria da declaração, desenvolve-se a teoria da confiança³³⁴. A teoria da confiança no negócio jurídico advém da perspectiva de Karl Larenz sobre o tema. Como explica Baggio, para o ilustre autor alemão, o negócio jurídico é um comando concreto no qual o ordenamento jurídico reconhece efeito vinculante. Assim, obrigam-se as partes a cumprir o contrato, não apenas porque resulta de sua manifestação de vontade, mas porque há um verdadeiro interesse da sociedade, seja pela segurança jurídica, seja pelos efeitos econômicos e sociais. Para Canaris, a aplicação da teoria deve preencher pressupostos essenciais como a) o *tatbestand*, b) a boa-fé do confiante, c) uma confiança objetiva e não desvairada e d) a responsabilidade pela confiança despertada³³⁵.

Andreza Baggio analisa a teoria da confiança com base nos estudos sobre os negócios jurídicos, entendendo a teoria como intermediária entre as teorias da vontade e da declaração. Dessa forma, a lei deve favorecer determinados interesses sociais do negócio e do contrato, valorizando a confiança dos contratantes e suas legítimas expectativas, que nascem de atos de

(expressão de Raizer)” (SCHMIDT NETO, André Perin. *Contratos na sociedade de consumo*: vontade e confiança. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*, cap. 3).

³³³ BAGGIO, *op. cit.*, p. 91.

³³⁴ “Assim, a teoria da confiança é tida como um ‘rebento’ ou uma criação resultante dos estudos sobre as teorias da vontade e da declaração. Segundo a teoria da confiança, a segurança jurídica dos negócios jurídicos se faz pela proteção da confiança no que foi declarado, pensamento que permitiu justificar a força vinculante de um contrato nas situações em que não havia vontade interna de modo que prevalece a declaração porque o declarante deve assumir a responsabilidade pela confiança que gera” (*Ibid.*, p. 93).

³³⁵ “A proteção da confiança, ou o chamado princípio da proteção da confiança no direito alemão, foi estudado por Claus Wilhelm Canaris, que desenvolveu o problema da responsabilidade pela confiança, em sua relação com a teoria da aparência, com a responsabilidade civil e boa-fé. Para o autor, são pressupostos necessários à proteção da confiança: a) o pressuposto fático da confiança (o *tatbestand*); b) a boa-fé [e daquele que confia]; c) a objetivação da confiança a ser protegida em certa medida; e d) a responsabilidade pela confiança despertada. Para o autor, a responsabilidade pela confiança, por sua vez, manifesta-se por meio da responsabilidade pela aparência, na responsabilidade pela confiança como imperativo ético-jurídico e na responsabilidade por declarações” (*Ibid.*, p. 94).

uma das partes. Protege-se, assim, a confiança na postura e nas obrigações assumidas por meio de suas declarações³³⁶.

Para Claudia Lima Marques, a teoria da confiança é um abrandamento da teoria da declaração porque confere maior valor à vontade declarada do que à interna, preservando a segurança nas relações contratuais e seus efeitos³³⁷. Baggio entende que a teoria da confiança é fruto de um aprimoramento das teorias da vontade e da declaração³³⁸.

Além disso, segundo Baggio, “encontrar na proteção da confiança a força vinculante do contrato é seguir uma teoria da declaração mitigada, pois neste pensamento protegem-se a segurança e a necessidade de não enganar a confiança legítima das partes e de terceiros nas manifestações externas”³³⁹. Baggio adverte: com os estudos sobre a formação dos negócios, percebeu-se que determinadas situações merecem tutela não apenas pela declaração da manifestação interna, mas também pela confiança provocada por uma das partes, pelas expectativas geradas³⁴⁰. A confiança tornou-se, então, um princípio geral do direito privado em diversos países do mundo, logrando uma posição importante para análise de diversos casos concretos³⁴¹.

A teoria da confiança é muito importante para o direito consumerista nacional, pois nota-se que o CDC protege amplamente a confiança do vulnerável em diversas etapas dos negócios, inclusive, na fase pré-contratual. Não é por acaso que Miragem ensina que a confiança é um dos mais importantes princípios do direito privado³⁴². Assim sendo, a partir da ideia da confiança como um imperativo ético-jurídico, visa-se analisar a importância da aplicação da teoria para proteger as legítimas expectativas de segurança dos consumidores nos contratos de tratamento de dados. A teoria da confiança possibilita uma interpretação mais favorável desses negócios jurídicos, colocando esse valor como força vinculante do contrato.

³³⁶ *Ibid.*, p. 92.

³³⁷ MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p. 212.

³³⁸ BAGGIO, *op. cit.*, p. 93.

³³⁹ *Ibid.*, p.120.

³⁴⁰ *Ibid.*, p. 93.

³⁴¹ “O respeito à confiança tornou-se um princípio geral, ultrapassando a fase em que o direito dele tratava incidentalmente. Passou a prevalecer tanto na área privada quanto no setor público, sendo objeto de tratados, leis e decisões jurisprudências em vários países” (SCHMIDT NETO, André Perin. *Contratos na sociedade de consumo: vontade e confiança*. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*, cap. 3).

³⁴² “A proteção da confiança é, atualmente, um dos mais importantes princípios do direito privado. Embora possa parecer paradoxal, em alguma medida isto se dá em razão de uma crise de confiança pela qual passa a sociedade de informação, cuja hipercomplexidade e hiperinformação dão conta de uma ruptura na crença em comportamentos tradicionais, em comportamentos padrões, reclamando-se a necessidade de estabelecimento da garantia da aplicação e efetividade do direito, por intermédio da proteção da confiança individual e social” (MIRAGEM, Bruno. *Curso de direito do consumidor*. 4. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2013, p. 229).

Desse modo, a observância da boa-fé e da confiança torna-se um requisito de validade dos negócios jurídicos, aferindo, especialmente, o cumprimento da função social do contrato.

2.3.2.3 A relação entre boa-fé, confiança e função social do contrato

A boa-fé é um instituto do Código Civil de 2002, prevista no seu artigo 422, que dispõe: “Os contratantes são obrigados a guardar, assim na conclusão do contrato, como em sua execução, os princípios de probidade e boa-fé”. A boa-fé serve como um norte na aplicação da legislação e na execução dos contratos, auxiliando o aplicador da lei na interpretação dos diplomas do ordenamento jurídico, como nas relações de consumo.

A palavra “boa-fé” é oriunda da expressão latina *fides*, que remete à ideia de fidelidade, de respeito da expectativa alheia, de honestidade e confiança³⁴³. Karl Larenz explica que a boa-fé compõe a confiança, sendo seu fundamento. A boa-fé (*Treu und Glauben*), segundo o autor, significa que cada um deve cumprir a própria palavra dada, que a confiança (*Vertrauen*) representa o fundamento vital de toda relação humana. Por conseguinte, esse valor não pode ser frustrado ou mal utilizado. Em cada relação humana, existe uma certa crença no modo como a pessoa irá agir e no que se pode esperar legitimamente da sua postura³⁴⁴.

Em relação à boa-fé, é preciso lembrar que existe a faceta objetiva e a subjetiva. A faceta subjetiva diz respeito ao aspecto íntimo do sujeito, suas considerações sobre o que acredita ser moral. Por isso, como o próprio nome sugere, é abstrata, de difícil padronização. Já a faceta objetiva da boa-fé está ligada a padrões de condutas aceitáveis na sociedade, vinculados à ética na vida em comunidade. A perspectiva objetiva estabelece *standards* de comportamento, como não enganar, ludibriar ou extorquir alguém, por exemplo.

A partir da consolidação de padrões de comportamento, a boa-fé objetiva instiga obrigações principais entre as partes e, também, conexas. Nesse sentido, a confiança atuará em parceria com a boa-fé, às vezes, até se complementarão³⁴⁵. Desse modo, ambos os princípios promovem uma cooperação entre as partes, visando o melhor desenvolvimento da relação contratual. Com efeito, o artigo 4.º, III, do CDC salvaguarda a boa-fé nas relações de consumo, apontando que os atores do mercado de consumo devem possuir relações harmônicas e pautadas pela boa-fé.

³⁴³ COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais*. 3. ed. São Paulo: Revista dos Tribunais, 2019, p. 76.

³⁴⁴ LARENZ, Karl. *Metodologia da ciência do direito*. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 1997, p. 291.

³⁴⁵ BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 111-112.

Para Fernando Noronha, tanto a boa-fé objetiva como a subjetiva servem para proteger a confiança, podendo a objetiva ser entendida como a boa-fé da confiança³⁴⁶. Miragem explica que a boa-fé possui três funções básicas, que são: a) princípio de interpretação e de integração dos negócios jurídicos, b) limite ao exercício de direitos subjetivos e c) fonte autônoma de deveres jurídicos³⁴⁷.

Em relação à função social do contrato, Miragem ressalta que esse princípio é reconhecido como fonte de novos efeitos dos contratos, alcançando, inclusive, terceiros. Nota-se uma complementaridade entre a boa-fé e a função social do contrato, ainda mais quando aliadas à proteção da confiança³⁴⁸. Miragem salienta que a importância da observância desses princípios deve-se ao fato de que o seu descumprimento pode acarretar a nulidade de cláusulas ou do contrato³⁴⁹.

Portanto, quem age de boa-fé protege a confiança. Verifica-se, desse modo, a proteção da confiança no Código Civil por meio do princípio da boa-fé objetiva, o que resulta em deveres de conduta principais e anexos entre as partes. Resta claro que, para o CDC, a boa-fé serve para proteger a confiança, exigindo das partes o cumprimento das obrigações assumidas, como as normas de conduta e os deveres de informação³⁵⁰. Com efeito, há uma relação natural entre a confiança e a função social do contrato, isto é, o instrumento de circulação de bens e serviços deve ser entendido a partir dos princípios da vulnerabilidade e da solidariedade.

A Constituição Federal exerce grande influência no CDC, especialmente na promoção da solidariedade e da justiça social, compreendendo que os contratos de consumo possuem o condão de inclusão ou exclusão social. Após a era do dogma da vontade, quando o *animus* era o único elemento vinculante do contrato, estuda-se o uso desse instrumento por meio da boa-fé, da função social e da proteção das legítimas expectativas que nascem da contratação³⁵¹.

³⁴⁶ NORONHA, Fernando. *O direito dos contratos e seus princípios fundamentais: autonomia privada, boa-fé, justiça contratual*. São Paulo: Saraiva, 1994, p. 136.

³⁴⁷ MIRAGEM, Bruno. Diretrizes interpretativas da função social do contrato. In: MIRAGEM, Bruno; MARQUES, Claudia Lima (org.). *Doutrinas essenciais: Direito do Consumidor*. São Paulo: Revista dos Tribunais, 2011. v. 1, p. 133.

³⁴⁸ “Já a função social dos contratos tem sido reconhecida entre nós, como fonte para o reconhecimento de novos efeitos aos contratos. E naquilo que se distingue da boa-fé, vai se revelar sobretudo pela geração de efeitos a outros sujeitos que não os contratantes (eficácia perante terceiros), tese cuja origem remonta ao direito francês, e que no Brasil teve sua divulgação a partir de um conhecido parecer do professor Antônio Junqueira Azevedo, cujo resultado determina a flexibilização do clássico princípio da relatividade dos contratos” (*Ibid.*, p. 134).

³⁴⁹ “Por fim, é preciso lembrar que o descumprimento da função social do contrato dará causa, sobretudo, a duas sanções específicas, quais sejam, a nulidade da cláusula ou do contrato que a violem, por força do estabelecido no art. 2.035, parágrafo único, do CC/2002, assim como imputação do dever de indenizar de quem a tenha violado em face de dano decorrente desta violação” (*Ibid.*, p. 135).

³⁵⁰ BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 113.

³⁵¹ *Ibid.*, p. 101.

A manifestação da vontade, sem dúvida, é um ponto de análise importante, contudo, não é o único critério nesse novo cenário, sendo importante compreender os efeitos da contratação, as condições econômicas e sociais. De fato, após a constitucionalização do direito privado, o contrato é um instrumento de justiça social que visa garantir a dignidade do consumidor.

Com a constitucionalização, o contrato, que era visto apenas como um instrumento de circulação de bens e serviços, agora começa a ser compreendido como uma ferramenta que garante a proteção do vulnerável, promovendo a segurança jurídica e a justiça social.

Percebe-se pelo exposto que existe uma relação entre confiança e função social do contrato. Assim, o contrato deve ser entendido com base nas expectativas geradas, da situação socioeconômica das partes, das assimetrias envolvidas naquele negócio, considerando a vulnerabilidade técnica-informacional tão patente nas relações de consumo.

Paulo Nalin explica que a funcionalização do contrato é fruto da abertura do direito civil a outras fontes jurídicas. A vontade, que já fora tida como o fundamento vinculante do contrato, hoje perde espaço para a boa-fé e a confiança entre as partes³⁵². A boa-fé, a confiança e a função social são verdadeiros limites à autonomia privada, que podem garantir uma ordem social harmônica entre os agentes do mercado. Nesse sentido, Baggio leciona “é possível entender que, para o Código de Defesa do Consumidor, a função social do contrato é proteger a confiança”³⁵³.

Ressalte-se que a função social do contrato caracteriza-se por ser uma cláusula aberta, com fundamento no artigo 170º da Constituição Federal e previsão no Código Civil, no artigo 421. Então, a partir de um diálogo de fontes, entre CF, CDC e CC, o contrato de consumo deve ser interpretado conforme sua função social, protegendo, assim, as legítimas expectativas do consumidor.

Claudia Lima Marques ensina que, nas relações de consumo, os *motivos da contratação* constituem *a causa de contratar* em razão das legítimas expectativas criadas no vulnerável. Esses motivos legítimos da contratação passam a integrar a relação contratual, o que impõe deveres de conduta aos contratantes, em especial, aos fornecedores³⁵⁴.

Consumir é um ato de confiança. O consumidor contrata um produto ou serviço que acredita suprir suas expectativas, de segurança ou de funcionalidade. Dessa maneira, o

³⁵² NALIN, Paulo. A função social do contrato no futuro Código Civil brasileiro. *Revista de Direito Privado*, São Paulo, v. 3, n. 12, p. 50-60, out./dez. 2002. 52

³⁵³ BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 101.

³⁵⁴ MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p. 110.

consumidor escolhe um determinado fornecedor por um motivo específico entre outros. Logo, aquela *causa de contratar* é essencial para aquele vínculo contratual. Assim, o consumidor possui expectativas naturais do que ele espera do serviço e daquele contratante. É importante que o ordenamento proteja essa confiança depositada, pois, em última análise, o ordenamento protege sua própria segurança jurídica.

Ensina Baggio: “Por esta razão, é certo dizer que a força vinculante do contrato baseia-se na busca por segurança jurídica, a qual se obtém pela tutela da confiança depositada na existência de certas situações de fato que criam legítimas expectativas”³⁵⁵.

Frada, ao falar sobre a proteção das expectativas no contrato, adverte: “a decisão de institucionalizar expectativas persegue então, na realidade, escopos que se situam para além da pura e *simples* tutela das expectativas: por exemplo, a institucionalização de quadros de segurança e fluidez no tráfego jurídico a proteção da parte mais fraca...”³⁵⁶.

Nota-se que a tutela da confiança visa garantir a estabilização de efeitos jurídicos e sociais por meio de padrões de comportamento socialmente éticos. Do exposto, extrai-se que a segurança jurídica no contrato de consumo será alcançada por meio da proteção da parte mais fraca, equilibrando uma relação desigual, o que pode ocorrer, por exemplo, pela tutela da confiança. A confiança torna-se, então, a verdadeira força vinculante do contrato³⁵⁷.

Com a massificação das relações de consumo e o novo paradigma tecnológico, verifica-se uma agravada vulnerabilidade do consumidor, sendo primordial a proteção da confiança como uma força obrigatória do contrato, como um fator de validade desse vínculo. Também é necessário levar em conta a supressão de autonomia de vontade na atualidade, especialmente no ciberespaço, pois o consumidor encontra-se em um estado de liberdade limitada, sujeitando-se aos serviços e produtos colocados no mercado pelos *players*. Essa liberdade limitada é fruto dos contratos de adesão, que suprimem as vontades dos consumidores e as possibilidades de negociação. Logo, a vontade, que já foi a força vinculante do contrato, hoje é totalmente dirimida em razão dos contratos padronizados de adesão.

Refletindo sobre essas mudanças, Claudia Lima Marques afirma que o contrato tem sofrido alterações e passado por crises ao longo do tempo. A autora sustenta que o direito contratual viveu e vive em crise. A primeira crise surgiu na Revolução Industrial em função da massificação das relações contratuais, o que resultou na supressão da autonomia privada,

³⁵⁵ BAGGIO, *loc. cit.*, p. 120.

³⁵⁶ FRADA, Manuel A. Carneiro da. *Teoria da confiança e responsabilidade civil*. Lisboa: Almedina, 2015. Reimpressão da edição de fevereiro de 2004. p. 362.

³⁵⁷ *Ibid*, p. 123.

porque os contratos de adesão tornaram-se o principal instrumento de circulação de bens e serviços. A segunda crise diz respeito à crise da pós-modernidade, em que os serviços e os bens imateriais assumem o centro das contratações. Já a terceira crise é a crise da confiança em virtude da crescente prestação de serviços de alta técnica e extrema complexidade, o que gera uma desconfiança dos consumidores em relação à segurança e à qualidade dos bens e serviços postos no mercado³⁵⁸.

As reflexões de Marques são certas e evidentes no dia a dia de um consumidor no ciberespaço. Absolutamente todos os contratos na *internet* são de adesão, no modelo *take it ou leave it*, e os serviços são o centro das contratações no ciberespaço, como serviços de armazenamento na nuvem, de *streaming* e outros.

Infere-se da análise de Marques que o contrato reflete as mudanças sociais, sendo um instrumento influenciado pelo comportamento da sociedade. Assim, em razão das novas realidades contratuais, o direito é instigado a dar respostas às crises. É nesse sentido que Bruno Miragem explica que há uma nova realidade contratual, que se caracteriza pela superação do dogma da vontade e pelo caráter absoluto da força vinculativa dos contratos. Além disso, ocorre o reconhecimento de novos deveres jurídicos entre os contratantes, como o respeito à boa-fé e a confiança³⁵⁹.

Pode-se dizer, portanto, que o consumidor atualmente enfrenta três crises contratuais ao consumir no ciberespaço. Não é à toa que Marques defende a importância da confiança como nova força vinculante do contrato, atuando de maneira complementar à boa-fé nesse novo paradigma tecnológico ao garantir as legítimas expectativas de segurança dos consumidores nas plataformas.

³⁵⁸ “A crise da massificação dos contratos levou alguns a afirmarem a ‘morte do contrato’, reabsorvido no *mainstream* dos atos ilícitos. A massificação dos contratos de adesão e das condições gerais contratuais foi o primeiro fenômeno de despersonalização do contrato, por meio de uma nova pluralidade e objetividade. Os consumidores são o exemplo desta pluralidade, mas também os fornecedores se organizaram em cadeias de fornecimento, não sendo sempre possível identificar com quem exatamente é a relação de consumo. Efetivamente, a dogmática contratual reagiu bem a esta primeira crise da era do consumo e impôs um novo paradigma repersonalizador, a boa-fé. Como afirmamos, boa-fé é a conduta que leva em consideração o outro, o pensar e respeitar lealmente as expectativas legítimas do outro, o fim que se visa na contratação. Boa-fé é informação, cuidado e cooperação, deveres hoje considerados anexos aos contratos de consumo. Agora estamos diante de um segunda crise, da despersonalização extrema. O ‘comércio eletrônico’ é realizado por intermédio de contratações à distância, por meios eletrônicos (*e-mail*), por internet (*online*) ou por meios de telecomunicação de massa (*telemarketing*, televisão, televisão a cabo etc.)” (MARQUES, Cláudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p. 64-65).

³⁵⁹ MIRAGEM, Bruno. Diretrizes interpretativas da função social do contrato. In: MIRAGEM, Bruno; MARQUES, Cláudia Lima (org.). *Doutrinas essenciais: Direito do Consumidor*. São Paulo: Revista dos Tribunais, 2011. v. 1, p. 133.

Nessa esteira, constata-se que o direito brasileiro possui fontes normativas capazes de tutelar a confiança do consumidor nas contratações no ciberespaço, como o CDC e a LGPD. Contudo, neste primeiro momento, importa demonstrar como o diploma consumerista é uma fonte primordialmente protetora da confiança, o grande vetor dessa teoria em solo nacional.

2.3.2.4 O Código de Defesa do Consumidor como fonte normativa protetora da confiança no ordenamento jurídico brasileiro

André Perin Schmidt Neto, em sua bela obra, ensina que a inclusão desses ensinamentos no Brasil ocorrera por meio do Direito Comercial e Administrativo³⁶⁰. É importante salientar que não há previsão expressa da proteção da confiança no ordenamento jurídico brasileiro, o que, por sua vez, não é nenhum óbice à proteção desse princípio³⁶¹.

Para deixar isso claro, basta ter em mente a defesa da privacidade pelo ordenamento nacional. Embora não haja menção expressa ao instituto, com base em uma série de interpretações sobre intimidade e vida privada, pode-se considerar que a privacidade é amplamente protegida no Brasil.

É importante ressaltar igualmente que a proteção da confiança em solo nacional também é assegurada no Código Civil³⁶². Observa-se, por exemplo, a proteção da confiança nos Enunciados n.º 362 e n.º 363, aprovados na IV Jornada de Direito Civil (2006), que visam a interpretação dos artigos 187 e 422 do Código Civil³⁶³.

³⁶⁰ “A confiança negocial – enquanto valor que embasa o princípio – já aparece na Gewere, figura da teoria do negócio jurídico estudada pelo jurista suíço Eugen Huber em 1894, mas que antes disso já era reconhecida no Direito europeu. No Brasil, a inclusão desse princípio no ordenamento jurídico se iniciou no Direito Comercial e no Direito Administrativo, uma vez que o Direito Privado adotou mais a doutrina alemã, resultando em maior utilização da expressão ‘confiança’, traduzida do alemão Vertrauens, enquanto no Direito Administrativo a introdução dessa ideia baseou-se na noção anglo-saxã de ‘legítimas expectativas’, tradução do termo legitimate expectations, motivo pelo qual é mais comum essa expressão para referir à mesma ideia, pois ambos partem da mesma noção. Essa proximidade entre as doutrinas não se dá apenas entre diferentes ramos do Direito, mas também em diferentes ordenamentos jurídicos, pois a doutrina da confiança é bastante homogênea no mundo todo, e isso se deve à indispensabilidade da presença desse valor para que seja possível o convívio social” (SCHMIDT NETO, André Perin. *Contratos na sociedade de consumo: vontade e confiança*. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*, cap. 3).

³⁶¹ “[...] mesmo não estando expressamente positivada, a confiança é adotada no Direito brasileiro” (SCHMIDT NETO, André Perin. *Contratos na sociedade de consumo: vontade e confiança*. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*, cap. 3).

³⁶² “Consagrada no Código Civil de 2002 a teoria da confiança, pode-se afirmar, com renovado vigor, que na interpretação das diversas cláusulas de um contrato devem-se considerar vinculantes os deveres que, manifestados pelas partes, suscitam em ambas uma compreensão comum quanto ao conteúdo da declaração” (SCHMIDT NETO, *loc. cit.*).

³⁶³ MARTINS, Rafael. Apontamentos sobre a confiança legítima no Direito brasileiro. *Revista da EMERJ*, Rio de Janeiro, v. 10, n. 40, p. 177-190, 2007. p. 189. Disponível em: <https://core.ac.uk/download/16041019.pdf>. Acesso em: 09 Fev 2023.

O Enunciado n.º 362 dispõe: “A vedação do comportamento contraditório (*venire contra factum proprium*) funda-se na proteção da confiança, tal como se extrai dos arts. 187 e 422 do Código Civil”. A denominada *venire contra factum proprium* é a vedação de mudanças inesperadas, impedindo comportamentos contraditórios, sendo um instituto alicerçado nos princípios da solidariedade e da confiança³⁶⁴. Por sua vez, o Enunciado n.º 363 assevera: “Os princípios da probidade e da confiança são de ordem pública, estando a parte lesada somente obrigada a demonstrar a existência da violação”.

Embora o CC/2002 tutele a confiança, é o CDC que se caracteriza por ser uma fonte normativa protetora desse princípio. A tutela da confiança pelo CDC é apenas um desdobramento natural dos novos ensinamentos desse diploma para a ordem jurídica nacional. Com efeito, a promulgação do CDC causou impacto no ordenamento jurídico brasileiro. Na época, em 1990, o Código Civil vigente ainda era o de 1916, um diploma ultrapassado para os novos ditames da justiça social e da solidariedade. Com a entrada em vigor do CDC, dois anos após a Constituição Cidadã, há a implementação de novos entendimentos no ordenamento jurídico, como, por exemplo, a consideração de vulnerabilidade do consumidor – um claro dirigismo contratual em relações privadas.

Portanto, o CDC é uma legislação fortemente influenciada pela Constituição Federal, incorporando os ditames de justiça social, solidariedade e dignidade do indivíduo. É nesse momento que existe uma quebra de paradigma na mudança de um Estado Liberal para o Estado Social. Essas novas perspectivas são evidenciadas, por exemplo, na compreensão do consumidor. Antigamente, as relações de consumo eram regidas pelo Código Civil de 1916, diploma que entendia o consumidor como um *Homo economicus*, cuja vontade era um dogma supremo, por mais que as causas e as consequências do negócio fossem catastróficas. Com o CDC, o consumidor é entendido, presumidamente, como um vulnerável. Logo, considera-se que existe uma assimetria de poder, de informação, de capacidade postulatória, entre outras, entre o consumidor e o fornecedor.

Em razão de tamanhas assimetrias, é instituído o microssistema de defesa do consumidor, com normas e princípios próprios que visam tratar o vulnerável de forma diferenciada. Assim, considera-se o consumidor como uma figura com potencial para ser manipulado, por carência de informações, de poder ou pelas influências comportamentais difundidas pelo *marketing*. Em razão do cenário de hipervulnerabilidade do consumidor no

³⁶⁴ BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 146.

ciberespaço, entende-se que o CDC é competente para proteger amplamente as legítimas expectativas do usuário, inclusive em fases pré-contratuais.

Os princípios da informação e da transparência³⁶⁵ (CDC, art. 4.º) são os pilares da proteção da confiança em fase pré-contratual, como nos casos da oferta e da publicidade. Se houver violação desses fundamentos, haverá um dano, que resultará em uma ação de responsabilidade civil³⁶⁶. No plano da oferta (CDC, art. 30³⁶⁷ e art. 31³⁶⁸), atesta-se a importância do princípio da informação e a existência de uma vinculação do preço publicizado com o público, se houver divergência com o que consta no sistema da loja ou na etiqueta.

Como ensina Baggio, o cumprimento vinculante da oferta relaciona-se com a proibição do comportamento contraditório, ressalvadas, assim, a boa-fé e a confiança do consumidor naquela proposta³⁶⁹. Dos exemplos citados, extrai-se que o CDC instituiu uma responsabilidade civil pré-contratual e preocupa-se com os efeitos da contratação, como, por exemplo, a tutela da confiança do vulnerável em relação à segurança e à qualidade dos produtos e serviços.

A confiança desempenha um papel fundamental na possibilidade de adequação do serviço às legítimas expectativas do consumidor, um papel essencial quando se leva em consideração que os contratos no ciberespaço, em sua maioria, são de adesão³⁷⁰. Desse modo, o CDC protege a confiança no ordenamento jurídico de duas maneiras distintas: aferindo a vinculabilidade entre as partes, buscando um equilíbrio contratual, e garantindo a possibilidade de adequação do produto ou serviço às legítimas expectativas do consumidor. Com base nessas suas facetas, observa-se claramente a ampla proteção da confiança pelo diploma.

Vale também destacar a proteção da confiança do consumidor em relação à propaganda enganosa e abusiva, visto que o CDC obriga o fornecedor a indenizar o consumidor apenas pela veiculação da publicidade com tais características. Tutela-se, assim, a confiança depositada pelo

³⁶⁵ “A transparência nos contratos de consumo pode ser vista como um direito do contratante mais fraco ou como um dever imposto ao contratante mais forte, que leva do dever de informar lealmente ao dever de transparência contratual ou informação” (MARQUES, Claudia Lima. *Contratos no Comércio... loc. Cit.*, p. 244).

³⁶⁶ BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 126.

³⁶⁷ “Art. 30. Toda informação ou publicidade, suficientemente precisa, veiculada por qualquer forma ou meio de comunicação com relação a produtos e serviços oferecidos ou apresentados, obriga o fornecedor que a fizer veicular ou dela se utilizar e integra o contrato que vier a ser celebrado”.

³⁶⁸ “Art. 31. A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores”.

³⁶⁹ “Ao determinar o cumprimento da oferta, o Código de Defesa do Consumidor acata o princípio da boa-fé e a proibição do comportamento contraditório, o chamado *venire contra factum proprium*” (BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 130).

³⁷⁰ *Ibid.*, p. 126

consumidor na informação prestada pelo fornecedor, ficando claro que o CDC adota a teoria da confiança nos seus artigos 30 a 35, dispositivos que tratam da oferta e da publicidade³⁷¹.

Para Claudia Lima Marques, o CDC apresenta-se como uma norma imperativa ética, protegendo a confiança do consumidor depositada no vínculo contratual. Segundo a autora, a confiança assume o papel de adequar o serviço ou produto às expectativas do consumidor, no que diz respeito à segurança e à usabilidade do produto ou serviço³⁷².

Seguindo essa linha, Baggio observa que os artigos 8.º, 9.º e 10.º proíbem produtos que causem danos aos consumidores, impedindo que sejam postos no mercado de consumo. Para a autora, essas disposições tutelam a confiança da coletividade consumidora ao garantir a qualidade e a adequação do serviço ou produto. O CDC apresenta *uma teoria da qualidade*, protegendo a incolumidade física e econômica do vulnerável³⁷³.

Baggio salienta: “Esta teoria da qualidade, que se estende também aos serviços de consumo, é informada pelo princípio da confiança, que, portanto, fundamenta todo o sistema de responsabilização civil do Código de Defesa do Consumidor”³⁷⁴.

Além disso, é importante destacar que o CDC é enfático em proteger o consumidor nos casos de abuso de direito, como se evidencia na proteção contra as práticas abusivas –outro caso prático de proteção das legítimas expectativas do vulnerável. Normalmente, as violações nos contratos de consumo decorrem do abuso da confiança depositada no vínculo, assim, os fornecedores impõem suas vantagens competitivas ao vulnerável, dando origem à figura do abuso de direito.

Para Baggio, o CDC, ao preocupar-se em evitar que o consumidor sofra alguma lesão, em sua incolumidade ou financeira, protege a confiança social nos produtos e serviços postos no mercado³⁷⁵. A autora sustenta que o CDC é uma norma protetora da confiança, comungando com os ensinamentos de Claudia Lima Marques. Baggio explica que o CDC “privilegia a manutenção do contrato em detrimento da sua extinção, sendo esta a verdadeira tutela da confiança à vulnerabilidade do consumidor, pois leva em consideração a sua dependência e

³⁷¹ *Ibid.*, p. 134.

³⁷² MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016, p.1346.

³⁷³ “Há, de acordo com o sistema do Código, uma verdadeira garantia legal de adequação de produtos e serviços, que cria, portanto, expectativas legítimas do consumidor quanto à sua observância, e, para respeitar a confiança do consumidor, o Código de Defesa do Consumidor apresenta uma teoria da qualidade, cujo objetivo é a sua incolumidade física e econômica” (BAGGIO, *op. cit.*, p. 136).

³⁷⁴ *Ibid.*, p. 137.

³⁷⁵ “Neste sentido, importa salientar que o abuso de direito no direito do consumidor se dá, normalmente, por meio do abuso na confiança depositada no cumprimento do contrato, razão pela qual o tema deve ser tratado em sua relação com a confiança, e não apenas em relação à boa-fé objetiva” (*Ibid.*, p. 149-150).

catividade”³⁷⁶. Verifica-se, de forma clara, a relação entre a necessidade de proteção da confiança do consumidor e a sua vulnerabilidade, pois tutelar as legítimas expectativas é proteger a vulnerabilidade do consumidor.

Segundo Marques, é preciso compreender o consumidor no contexto atual; em outras palavras, é preciso entender a sociedade de consumo tecnológica, voltada para a produção de serviços hiperespecializados e desmaterializados, que são estimulados pelo *marketing* agressivo e por outras formas de modulação de comportamento. Constata-se, assim, que a manifestação de vontade não é livre, é limitada pela oferta, pelas necessidades de contratação e pela catividade³⁷⁷.

A proteção da confiança do consumidor nada mais é, portanto, do que a tutela da sua vulnerabilidade no mercado de consumo. A garantia do respeito às legítimas expectativas do vulnerável ocorre tanto na fase de aproximação negocial, como na execução do contrato, como demonstrado. Na fase de execução do contrato, a confiança terá o importante papel de adequar o serviço às expectativas iniciais de segurança³⁷⁸.

O mercado de consumo é um excelente ambiente para aferir a importância da confiança. Com efeito, nas palavras de Baggio, o consumidor “precisa crer nas informações recebidas e no respeito à qualidade prometida, e confiar que aquele produto não colocará em risco a sua vida e a vida de seus familiares, precisa confiar que o contrato firmado será cumprido pelo fornecedor”³⁷⁹. A confiança é decorrência natural da vulnerabilidade, pois o vulnerável não tem acesso às informações completas, apenas as recebe dos fornecedores, cabendo ao consumidor confiar em que o produto ou serviço é seguro.

“Pode-se então dizer que o Código de Defesa do Consumidor é hoje um grande instrumento de tutela da confiança nas relações negociais dentro do ordenamento jurídico brasileiro, e que os contratos de consumo são verdadeiros negócios de confiança”³⁸⁰. Assim, realizando um diálogo de fontes – teoria proposta por Erik Jayme e difundida por Claudia Lima Marques em solo nacional –, é possível, por meio do CDC e do CC, proteger as legítimas expectativas de consumidores.

Claudia Lima Marques defende de maneira cristalina a proteção da confiança pelo CDC. Vai além, sustentando que a tutela da confiança no comércio eletrônico é essencial, devendo

³⁷⁶ *Ibid.*, p. 119.

³⁷⁷ MARQUES, Claudia Lima. *Contratos no comércio.. Op. Cit.*, p. 64 et seq.

³⁷⁸ BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012, p. 97.

³⁷⁹ BAGGIO, *loc. cit.*

³⁸⁰ *Ibid.*, p. 99.

assumir um novo patamar para a proteção dos vulneráveis em um espaço desterritorializado, desmaterializados e despersonalizado.

Como ensina Marques, “parece haver um consenso universal de que o consumidor no comércio eletrônico deve receber o mesmo grau de proteção que já alcançou em seu país no comércio normal”³⁸¹. É imperativo, portanto, que o direito brasileiro tutele a confiança do usuário-consumidor no que tange a sua proteção de dados, valorizando os deveres de transparência, informação e responsabilidade dos fornecedores.

Desse modo, defende-se que a teoria da confiança difundida em solo nacional será o paradigma-mãe da boa-fé no comércio eletrônico quando se trata de contratos de tratamento de dados³⁸². Como diz André Perin Schmidt Neto, “não é absurdo ou meramente retórico, portanto, afirmar que sem uma adequada proteção da confiança legítima o sistema jurídico sequer está cumprindo seu papel”³⁸³.

Por meio de um diálogo de fontes, entre o CDC e a LGPD, previsto inclusive no artigo 45 da LGPD, é plenamente possível analisar os contratos de tratamento de dados à luz da teoria da confiança, atuando positivamente e negativamente na proteção do vulnerável. Portanto, a teoria que surgiu no século XX mostra-se valiosa para dirimir problemáticas complicadas em relação à proteção de dados no ciberespaço.

³⁸¹ MARQUES, Claudia Lima. *Contratos no comercio... Op. Cit.*, p.152.

³⁸² “Considerarei aqui que a confiança é o paradigma-mãe da boa-fé, pois na definição mesmo de *bona fides*, a *fides* já é elemento pré-definidor” (*Ibid.*, p. 153).

³⁸³ “Não é absurdo ou meramente retórico, portanto, afirmar que sem uma adequada proteção da confiança legítima o sistema jurídico sequer está cumprindo seu papel. Afinal, o homem que confia, necessariamente, coloca-se numa posição mais frágil e vulnerável, dentro de determinada relação jurídica. Para compensar esta vulnerabilidade, cabe ao ordenamento jurídico garantir um mínimo de segurança para o desenvolvimento das atividades do indivíduo” (SCHMIDT NETO, André Perin. *Contratos na sociedade de consumo: vontade e confiança*. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*, cap. 3).

3 A PROTEÇÃO DE DADOS PESSOAIS À LUZ DA TEORIA DA CONFIANÇA

É evidente que o consumidor encontra-se em um estado de hipervulnerabilidade diante de todos os riscos presentes no ciberespaço, ainda mais agravado em razão da confiança sistêmica influenciada pelas plataformas. A abissal disparidade entre usuário e plataforma impõe a necessidade de um aprimoramento da tutela das legítimas expectativas de proteção de dados dos usuários no cenário nacional.

Para Szafir e Hillary, a vulnerabilidade do consumidor é decorrente da debilidade para negociar com o fornecedor com paridade de armas³⁸⁴. Como ensinam Marques e Miragem, não importa se o consumidor é analfabeto ou pós-doutor, a vulnerabilidade é uma presunção absoluta de todos os consumidores por ser a relação de consumo, em sua própria natureza, desequilibrada³⁸⁵.

Em razão de tamanha disparidade, observa-se em casos concretos a figura do consumidor hipervulnerável. De acordo com Szafir e Hillary, a hipervulnerabilidade é subjetiva e relacional, sendo o reflexo de diversos fatores, sociais, culturais, fáticos, econômicos, técnicos, informacionais e comportamentais, entre outros³⁸⁶. Observa-se que no mundo digital, o consumidor enfrenta diversas vulnerabilidades, como a econômica, jurídica, técnica-informacional, algorítmica e comportamental, que o colocam em um estado de hipervulnerabilidade, sendo a parte mais débil na negociação.

A vulnerabilidade é o fundamento que garante a proteção da *fides* do consumidor nas relações de consumo. Portanto, quanto maior a vulnerabilidade mais é imperativo a proteção das legítimas expectativas do consumidor. Neste sentido, compreende-se que é fundamental a

³⁸⁴ “En las últimas décadas la dicotomía entre la autonomía de la voluntad y el intervencionismo legal en materia contractual ha sido resuelto en favor del débil negocial, esto es, el sujeto vulnerable, en aras de defender la igualdad de las partes en las relaciones jurídicas, así como valorar la justicia en las soluciones legales ya que los principios rectores del derecho decimonónico ‘autonomía de la voluntad’ y ‘pacta sunt servanda’ ya no pueden cumplir su misión. En efecto, para que el principio de autonomía de la voluntad sea el rector de las relaciones entre los sujetos, debemos contar con partes que tengan el mismo poder de negociación, esto es, un pacto entre iguales desde el punto de vista jurídico, económico, social y cultural. El desarrollo de la contratación en masa y la proliferación del marketing han permitido que los proveedores tengan un poderío que desequilibra la relación, en perjuicio del consumidor afectado por su debilidad o vulnerabilidad” (SZAFIR, Dora; MARKS, Hillary. Consumidores hipervulnerables: ¿necesidad de mayor protección? *Revista de Direito do Consumidor*, São Paulo, v. 31, n. 139, jan./fev. 2022, p. 52-53).

³⁸⁵ “Do princípio da vulnerabilidade previsto no art. 4.º, I, retira-se uma presunção (legal) absoluta de vulnerabilidade do consumidor, seja rico ou pobre, analfabeto ou pós-doutor, qualquer consumidor ou sujeito de direito qualificado como consumidor é vulnerável” (MARQUES, Claudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. São Paulo: Revista dos Tribunais, 2014, p. 197-198):

³⁸⁶ “Esta condición es subjetiva y relacional, por lo que el mero hecho de pertenecer a una categoría no lo convierte en tal. Lo será en caso de encontrarse en cierta condición que lo lleve a una mayor debilidad frente al proveedor. La hipervulnerabilidad no refiere a un solo factor, sino que puede tratarse de la coexistencia de varios factores: sociales, culturales, fáticos, económicos o de salud” (SZAFIR; MARKS, *op. cit.*, p. 53):

proteção da confiança em uma outra dimensão no ciberespaço, visto que esse ambiente é permeado por esse valor, pois como reflete Mucelin “quanto maior à distância e a impessoalidade do fornecedor, torna-se mais importante buscar a confiança do consumidor³⁸⁷”.

Os milhares de contratos firmados, minuto a minuto no ciberespaço, são a materialização da confiança, da *fides* de que mesmo uma plataforma que possua sede no outro lado do oceano cumprirá o contrato firmado, especialmente a obrigação de proteção dos dados pessoais. Um ambiente como o ciberespaço, onde ninguém conhece ninguém, mas todos se relacionam³⁸⁸ e contratam, só é possível graças a uma confiança sistêmica.

Desses vínculos firmados na *internet* surgem legítimas expectativas de privacidade por parte dos titulares. Sendo assim, o usuário confia que as obrigações pactuadas, como de proteção de suas informações pessoais, serão cumpridas, garantindo sua segurança. Com a proteção da confiança pelo CDC e Código Civil, sua tutela ultrapassa a questão ética para torna-se um imperativo contratual³⁸⁹. Dessa forma, obrigam-se as partes a agirem conforme a boa-fé e respeito as legítimas expectativas, especialmente, quando existir disparidades na relação, evitando-se que uma das partes, mormente a vulnerável, crie representações falsas ou temerárias³⁹⁰.

Ressalte-se que a sociedade se encontra em uma era de consumo excessivo, estimulado pelos fornecedores. Nessa sociedade do consumo, a confiança é depositada no *branding*, como explica Lipovetsky ao elucidar que a fiabilidade não se encontra mais em um dado comerciante, mas está na referência simbólica e institucional da marca, a garantia e a qualidade sendo transferidas dos produtos para o fabricante. Dessa forma, o consumo ocorre sem o intermédio do negociante, e o consumidor orienta-se a partir da marca e de seu nome, o que revela uma ligação entre marca e confiança para o consumidor³⁹¹.

Com efeito, no novo paradigma tecnológico e no contexto do capitalismo de vigilância, a confiança agora reside nas plataformas³⁹². Não sendo exagero dizer que hoje os consumidores

³⁸⁷ MUCELIN, Guilherme. *Loc.cit [e-book, cap 3]*.

³⁸⁸ *Ibid.*

³⁸⁹ AZEVEDO, Ricardo. O legítimo interesse e a legítima expectativa do titular dos dados pessoais. In: OLIVEIRA, Ricardo; COTS, Márcio, coordenação. *O legítimo interesse e a LGPD*. 2. Ed. Ver., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021. p. 115-116.

³⁹⁰ *Ibidem*, p. 119: Portanto, as condutas impostas pela boa-fé às partes de uma relação jurídica, principalmente quando na relação existe uma disparidade de forças, inserem-se na exigência de não suscitar ou sustentar indevidamente a confiança de outrem, evitando que a outra parte crie representações falsas ou temerárias.

³⁹¹ LIPOVETSKY, Gilles. *A felicidade paradoxal: ensaio sobre a sociedade de hiperconsumo*. São Paulo: Companhia das Letras, 2007, p. 30.

³⁹² VERBICARO, Dennis; CALANDRINI, Jorge. A proteção da confiança do consumidor e a base do legítimo interesse na Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). *Revista de Direito do Consumidor*, São Paulo, v. 31, n. 139, jan./fev. 2022, p. 77.

buscam utilizar serviços que protejam sua privacidade e dados pessoais, sendo um dos *motivos* da contratação de uma plataforma em detrimento de outra.

Assim sendo, existe uma crença na tecnologia, que resulta em uma espécie de tecnocracia ou no que Van Dijck denomina “dataísmo”. Para a autora, o dataísmo é a confiança exacerbada na tecnologia, em seus criadores e nas agências de regulação, o que resulta em uma análise rasa dos riscos para a sociedade, gerando diversos desafios regulatórios para o direito.

3.1 A Confiança na Neutralidade das Plataformas

O início do *e-commerce* foi marcado por diversas desconfianças, muitas delas geradas pelas suas características principais: despersonalização, desmaterialização e despersonificação³⁹³. Como o consumidor estava distante do fornecedor, especialmente da figura do vendedor, e como era impossível o contato com o produto, o consumidor temia ser enganado ou receber um produto diferente do apresentado no *site*. Nesse momento, o comércio eletrônico apresentava-se como inovador, contudo, impregnado de desconfiança.

Após ações de *marketing* e a utilização cotidiana do comércio eletrônico pelos usuários, consolidou-se essa modalidade de consumo. O comércio eletrônico é objeto de uma *hiperconfiança* por parte dos consumidores, deixando-os cegos ou ignorantes dos riscos. A confiança sistêmica e exacerbada nas plataformas³⁹⁴ resulta em uma *crença* na neutralidade dos *players*.

Essa *hiperconfiança* só foi possível a partir de um investimento maciço das empresas em *marketing* e em segurança nas negociações no ciberespaço, com o objetivo de fortalecer o comércio eletrônico, transferindo confiabilidade a esse meio de consumo. Além desses investimentos pelas plataformas, para lograr a confiança dos consumidores no comércio eletrônico, o Estado também buscou fortalecer essa forma de consumo, como, por exemplo, o direito ao arrependimento estipulado no artigo 49 do CDC, que possibilita a desistência de produtos e serviços adquiridos em domicílio ou fora do estabelecimento comercial, como na *internet*.

³⁹³ MARQUES, Claudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*. São Paulo: Revista dos Tribunais, 2004.

³⁹⁴ “Ultrapassa-se, assim, de certa forma, a desconfiança geral que existe no mercado de consumo e, em especial, no que se refere ao comércio eletrônico tradicional, para uma fase pós-moderna de confiança generalizada, exacerbada, abundante, circular e sistêmica – o que Claudia Lima Marques convence chamar de *hiperconfiança*” (MUCELIN, Guilherme. *Conexão online e hiperconfiança: os players da economia do compartilhamento e o direito do consumidor*. São Paulo: Revista dos Tribunais, 2020. *E-book*, cap. 4).

O fortalecimento da confiança no comércio eletrônico fez com que a modalidade crescesse ano após ano. Por outro lado, com o crescimento do *e-commerce*, a confiança também progride. Contudo, é necessário estar atento à possibilidade de a *hiperconfiança* deixar o consumidor *hipervulnerável*, sem informações qualificadas e sem ciência dos riscos aos direitos de personalidade e de privacidade.

Pesquisadores sustentam que há uma *alienação técnica*³⁹⁵ no atual contexto tecnológico, limitando as reflexões sobre os riscos das inovações tecnológicas. Indo por esse caminho, Van Dijck lança o conceito de dataísmo. A autora explica que o conceito é uma desconstrução do conceito de datificação, proposto por Mayer-Schoenberger e Cukier, o qual, segundo Van Dijck, não responde a todas as problemáticas do atual estágio tecnológico³⁹⁶. O dataísmo, por sua vez, caracteriza-se por uma crença generalizada na quantificação objetiva e no rastreamento de todos os tipos de comportamento humano. Além disso, o dataísmo é possível, em grande parte, *pela confiança* nos agentes institucionais de coleta, tratamento e compartilhamento de dados³⁹⁷.

Sobre a relação entre dataísmo e confiança, Van Dijck esclarece:” Noções de ‘confiança’ e de ‘crença’ são particularmente relevantes quando se trata de entender a vigilância de dados: uma forma de vigilância contínua por meio do uso de (meta)dados”³⁹⁸. Há, portanto, uma intrínseca relação entre proteção de dados, confiança e dataísmo, não sendo por acaso que o presente trabalho se esforça por lançar luz sobre a necessidade de proteção da confiança nas relações de coleta e de tratamento de dados no ciberespaço.

Para demonstrar como os cidadãos confiam nas instituições que armazenam dados dos cidadãos para monitoramento, Van Dijck relembra o caso envolvendo Edward Snowden e a

³⁹⁵ “A alienação técnica, termo originariamente forjado pelo filósofo Gilbert Simondon, aqui é definida como a ignorância ativa sobre como funcionam as redes de criação, desenvolvimento e uso de tecnologias, na fé da completa ausência de importância de se conhecer e dominar localmente os processos tecnológicos” (SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021, p. 44):

³⁹⁶ VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigms and ideology. *Surveillance & Society*, [s.l.], v. 12, n. 2, p. 198.

³⁹⁷ “[...] the ideology of *dataism* shows characteristics of a widespread *belief* in the objective quantification and potential tracking of all kinds of human behavior and sociality through online media technologies. Besides, dataism also involves trust in the (institutional) agents that collect, interpret, and share (meta)data culled from social media, internet the (institutional) agents that collect, interpret, and share (meta)data culled from social media, internet platforms, and other communication technologies” (VAN DIJCK, *loc. cit.*, grifo do autor).

³⁹⁸ VAN DIJCK, *loc. cit.*, grifo do autor, tradução nossa. No original: “Notions of ‘trust’ and ‘belief’ are particularly relevant when it comes to understanding *dataveillance*: a form of continuous surveillance through the use of (meta)data”.

Agência de Segurança Nacional (NSA, na sigla em inglês)³⁹⁹. Defende-se aqui que tal entendimento deve estender-se às plataformas.

Van Dijck, ao relacionar o dataísmo com a confiança nas instituições, filia-se ao grupo de pesquisadores que ressaltam a importância da confiança dos usuários nas plataformas para que os procedimentos de aplicação com inteligência artificial e quantificação do comportamento, realizados por empresas, agências governamentais e outros, sejam pacificamente aceitos⁴⁰⁰. Ainda, para Van Dijck, a atitude dos acadêmicos que pressionam a regulação pelos Estados nacionais em função dos efeitos adversos da datificação nada mais é do que um modo de salientar a importância da confiança nessas relações, pois, ao pedir boa-fé e transparência, roga-se, em última análise, por um reforço da confiança nesses sistemas⁴⁰¹. Dessa maneira, Van Dijck leciona: “Na luta por confiança e credibilidade, há uma suposta separação do público, das instituições corporativas e estatais como órgãos autônomos, cada um tendo uma relação distinta com os usuários – consumidores ou cidadãos”⁴⁰².

Segundo Van Dijck, a suposta separação entre público e privado garante a confiança dos usuários nos sistemas peritos, fazendo com que a população acredite que os órgãos regulatórios dos governos realizarão suas funções. Contudo, no atual estágio, o que se verifica é a submissão dos Estados às grandes empresas de dados por diversos fatores, por dependência, economicamente ou até pela impossibilidade de impor sanções, visto que elas atuam de maneira globalizada, podendo migrar para qualquer país que aceite suas operações sem questionar.

Assim sendo, as plataformas buscam manter a fé dos usuários em suas políticas de dados, pois sabem que a proteção da privacidade hoje é uma vantagem competitiva, contudo, em razão da arquitetura desse negócio, as promessas das companhias revelam-se cada vez mais impossíveis de serem cumpridas em função do capitalismo de vigilância⁴⁰³. Van Dijck afirma que o dataísmo pressupõe a confiança nos métodos quantitativos, bem como na crença na independência e na integridade das instituições – governamentais ou plataformas corporativas.

³⁹⁹ “As Snowden’s documents made clear, people have faith in the institutions that handle their (meta)data on the presumption that they comply with the rules set by publicly accountable agents” (VAN DIJCK, *loc. cit.*).

⁴⁰⁰ “Data companies, government agencies and researchers alike underscore the importance of users’ trust in societies where growing parts of civilian life – from application procedures to medical records and financial transactions – are moved onto online platforms” (VAN DIJCK, José. *Datafication, dataism and dataveillance: Big Data between scientific paradigms and ideology. Surveillance & Society, [s.l.], v. 12, n. 2, p. 202*).

⁴⁰¹ VAN DIJCK, *loc. cit.*

⁴⁰² *Ibid.*, p. 203, tradução nossa. No original: “In striving for trust and credibility, there is a presumed separation of public, corporate, and state institutions as autonomous bodies that each has a distinctive relationship with users – whether consumers or citizen”.

⁴⁰³ “Data companies, for their part, are simultaneously competitors and allies when it comes to winning and keeping users’ trust. Users’ faith in their data policies may be part of a single company’s competitive edge; however, since partnerships in this sector abound it is impossible for users to keep track of who shares data with whom” (VAN DIJCK, *loc. cit.*).

Todavia, admite que as plataformas enfrentam dificuldades para respeitar a confiança e a independência que tanto propagam⁴⁰⁴.

Observa-se, por todo o exposto, que o ser humano tende a confiar nas tecnologias, no progresso. Essa crença na tecnologia é percebida na *hiperconfiança* nas plataformas, especialmente na *fides* de neutralidade econômica, política e até de interesses nacionais dos *players*⁴⁰⁵. Embora seja notória a *hiperconfiança* do consumidor nas plataformas, como muito bem adverte Van Dijck, o que está em jogo não é nossa confiança apenas nas plataformas ou nas agências governamentais, é a credibilidade de todo o ciberespaço e seus métodos⁴⁰⁶.

Citando outro exemplo de confiança exacerbada nas plataformas pelos usuários, Sérgio Amadeu da Silveira afirma que a *fides* no cumprimento dos contratos, mesmo quando a jurisdição para a resolução do conflito não é a nacional⁴⁰⁷, é a materialização da confiança sistêmica dos usuários, observada cotidianamente nas relações contratuais do ciberespaço.

Além da patente confiança nas plataformas, a imagem de neutralidade é explorada pelas empresas, inclusive no modo como se apresentam aos consumidores. Quase sempre os aplicativos do comércio eletrônico apresentam-se como *intermediários*, apenas como um facilitador de dois lados, eximindo-se de uma ingerência nas relações. Desse modo, as imagens das plataformas expressam uma neutralidade, que ofusca, por exemplo, sua interferência na modulação do conteúdo, na oferta e no controle dos meios de pagamento. Toda essa semântica linguística favorece uma ideia de neutralidade trabalhada minuciosamente pelas plataformas.

Os esforços envidados pelas plataformas mostram-se muito eficazes, pois é notável a confiança nos *players* pelos consumidores, que aceitam conceder seus dados pessoais para tratamento de informações, muitas vezes, de maneira ilegal. Nesse sentido, é necessário

⁴⁰⁴ “Dataism presumes *trust* in the objectivity of quantified methods as well as in the *independence* and *integrity* of institutions deploying these methods – whether corporate platforms, government agencies, or academic researchers. Trust and independence, however, are embattled notions in an ecosystem of connectivity where all online platforms are inevitably interconnected, both on the level of infrastructure as on the level of operational logic” (*Ibid.*, p. 204, grifo do autor).

⁴⁰⁵ “No nosso entusiasmo e crescente dependência da tecnologia, temos a tendência a esquecer que as mesmas forças do capital das quais havíamos fugido no mundo real estavam rapidamente reivindicando a posse da esfera digital, mais abrangente. Isso nos deixou vulneráveis e nos pegou desprevenidos quando a promessa inicial do capitalismo de informação sofreu uma guinada para o pior” (ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020, p. 63).

⁴⁰⁶ “What is at stake here is not simply our ‘trust’ in specific government agencies or single corporations, but the credibility of the entire ecosystem – an ecosystem that is fueled by a steady flow of billions of e-mails, video, text, sound, and metadata. The custody over data flows appears to be mired in a fuzzy delineation of territories; access and restrictions to data are fought over both before the public’s eye and outside people’s realm of knowing” (VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigms and ideology. *Surveillance & Society*, [s.l.], v. 12, n. 2, p. 204).

⁴⁰⁷ SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021, p. 46.

verificar que a confiança está agravando os riscos à tutela dos dados pessoais dos usuários, sendo necessário, portanto, que o direito proteja esse valor de maneira mais enérgica, valorizando os deveres de transparência, de informação e de responsabilização, garantindo um maior controle e autodeterminação aos usuários.

3.1.1 O investimento na confiança dos consumidores pelas plataformas: desde os modelos de negócio, mecanismos de classificação e práticas publicitárias.

Os modelos de negócios são a forma que as empresas utilizam para executar seu *business*. Como já explicado, há uma *plataformização da web*. Plataformas, em sua conceituação pacífica, são um negócio de dois ou mais lados, como os modelos de negócios dos *players* (*vide* capítulo 1).

A *plataformização* é o modelo dominante do ciberespaço, permitindo, por exemplo, a economia do compartilhamento e suas outras múltiplas expressões. Estabelece-se uma relação trilateral no ciberespaço, entre um consumidor, um fornecedor e uma plataforma intermediária. O papel da plataforma é ceder o espaço no seu *site*, realizar a publicidade do bem ou serviço e controlar a forma de pagamento. Do outro lado, existe um indivíduo que deseja o bem ou serviço – o consumidor – e um fornecedor – que, por não conseguir competir com os grandes *players* da *internet*, alia-se às suas plataformas.

O *marketplace* é um grande exemplo do descrito acima. Pequenos fornecedores, sem investimento e *expertise* técnica para construir um *site* e mantê-lo competitivo, migram para plataformas de grandes empresas para conseguir vender seus produtos e serviços. Para um restaurante, é muito mais viável ir para o *Ifood* do que criar sua própria plataforma e administrá-la, assim como é bem mais acessível para os motoristas de aplicativo aliarem-se ao *Uber* e afins.

Empresas como *Airbnb* revelam que seu modelo de negócio só é possível com base na confiança. Em 2019, o *CEO* da empresa compartilhou um *e-mail* com seus colaboradores intitulado “No negócio da confiança”, assinalando no primeiro parágrafo: “O negócio do Airbnb é movido pela confiança. Quando começamos em 2008, as pessoas falavam que nunca daria certo. ‘Estranhos nunca vão confiar uns nos outros’, diziam”⁴⁰⁸. Prosseguindo, o *CEO* afirmou que a empresa sempre acreditou que as pessoas são essencialmente boas e que, por

⁴⁰⁸ AIRBNB. No negócio da confiança. *News*, 6 nov. 2019. Disponível em: <https://news.airbnb.com/br/no-negocio-da-confianca/>. Acesso em: 23 out. 2022.

isso, poderia criar um *sistema* para estranhos *confiarem uns nos outros*. Além disso, concluiu, “a confiança é a verdadeira fonte de energia do Airbnb”⁴⁰⁹.

O *e-mail* da empresa é uma prova cristalina da concepção sociológica da confiança como um valor social. Além disso, é uma confirmação de que os modelos de negócios das plataformas são sustentados por uma confiança sistêmica e de que a segurança nas relações negociais é medida com base na confiança. Nesse modelo de negócio, por exemplo, o consumidor recorre a sistemas de classificação para escolher o pequeno fornecedor cujo produto deseja consumir⁴¹⁰. Os sistemas de classificação, criados pelas plataformas, visam incentivar o usuário a avaliar o produto e o serviço do fornecedor, o que inclui a apreciação do tratamento no primeiro contato, a qualidade do produto ou serviço ou o tempo de frete, por exemplo. Destaca-se, pois, a figura do *prosumer*.

Com efeito, o usuário avalia os comentários anteriores de outros consumidores, seus elogios e suas queixas. Todas essas informações têm o objetivo de assegurar a confiabilidade, porque o usuário verifica que outros indivíduos consumiram aquele bem daquele fornecedor e que a experiência foi satisfatória. Logo, os sistemas de classificação estimulam a confiança.

Observa-se, também, que o valor confiança é utilizado em ações publicitárias. Foi o que fez, por exemplo, a empresa Uber ao começar suas operações no Brasil. A Uber chegou ao Brasil com preços mais acessíveis do que os táxis convencionais. Havia, porém, uma grande desconfiança por parte dos passageiros, que temiam, por exemplo, possíveis assaltos. No início do funcionamento do aplicativo no Brasil, a empresa lançou a campanha “Segurança 5 estrelas”, na qual demonstrava que seus colaboradores passavam por um processo de avaliação antes de ingressar na empresa. Posteriormente, a Uber lançou a campanha “A confiança começa pelo nome”, assim, motoristas e passageiros, quando era pedida uma corrida, já sabiam os nomes uns dos outros. A diretora de *marketing* da empresa explicou o objetivo da campanha: “A experiência de saber com quem você está compartilhando sua viagem traz uma sensação de

⁴⁰⁹ “Mas nós acreditávamos que as pessoas são essencialmente boas, e que poderíamos *desenhar um sistema para estranhos confiarem uns nos outros*. Nossa verdadeira inovação não é permitir que as pessoas aluguem um espaço; é desenhar uma estrutura que permite que milhões de pessoas confiem umas nas outras. A confiança é a verdadeira fonte de energia do Airbnb e nos deu condições de expandir nossa plataforma para 191 países e mais de 600 milhões de membros” (AIRBNB, *loc. cit.*, grifo nosso).

⁴¹⁰ “Em outros termos, essa confiança, ou melhor, a hiperconfiança é a disposição das pessoas em cooperar em determinado sistema, mesmo que não se conheça os parceiros contratuais, como no caso do consumo compartilhado; é sopesar atuações passadas de internautas, não com base na proximidade, mas com base em todos os dados e informações pretéritos de comportamento estruturados em *scores*” (MUCELIN, Guilherme. *Conexão online e hiperconfiança: os players da economia do compartilhamento e o direito do consumidor*. São Paulo: Revista dos Tribunais, 2020. *E-book*. cap. 4).

confiança. E essa *confiança* começa a ser criada quando aprendemos os nomes uns dos outros”⁴¹¹.

Outros exemplos de grandes empresas que se preocupam em conferir confiança em seus negócios são as empresas da Facebook Inc., que inclusive contam com um cargo de chefe de política de confiança e segurança. O WhatsApp, no seu *site*, explica: “Simples. Seguro. Troque mensagens com *confiança*”.

O *Facebook*, após alguns escândalos, como os provocados pela *Cambridge Analytica* pela demora em conter conteúdos extremistas, reconhece que a plataforma sofre com um *déficit* de confiança. Neil Potts, chefe de política de confiança e segurança da empresa, reconheceu, em um vazamento de ligação, obtido pelo *Financial Times*, que a empresa não goza da confiança dos seus usuários⁴¹². O sentimento do funcionário da empresa é comprovado pela pesquisa chamada *Us Digital Trust Survey*, que avaliou fatores como legitimidade, segurança, experiência, relevância de anúncios e comunidade. A pesquisa aferiu que 32% dos usuários americanos acreditam que a empresa protege seus dados e sua privacidade – a menor porcentagem em comparação com outras redes sociais⁴¹³.

Empresas com ótimo índice de confiança dos consumidores têm-se esforçado para proteger os dados pessoais dos usuários. É o caso da *Apple* que comprou a briga dos usuários contra o *Facebook* ao permitir que o usuário escolha se o aplicativo pode ou não rastrear seus dados⁴¹⁴. Com efeito, a nova ferramenta tornou-se uma campanha publicitária sobre proteção de dados em seus aparelhos⁴¹⁵, com o intuito de diferenciar-se dos competidores ao demonstrar

⁴¹¹ NOVA campanha da Uber dá protagonismo às pessoas. *Promoview*, 17 maio 2018. Disponível em: <https://www.promoview.com.br/categoria/publicidade/nova-campanha-da-uber-da-protagonismo-as-pessoas.html>. Acesso em: 23 out. 2022.

⁴¹² FACEBOOK perde anunciantes e diz sofrer com “déficit de confiança”. *Canaltech*, 29 jun. 2020. Disponível em: <https://canaltech.com.br/publicidade/facebook-perde-anunciantes-e-diz-sofrer-com-deficit-de-confianca-167214/>. Acesso em: 23 out. 2022.

⁴¹³ AGRELA, Lucas. Facebook é último colocado em ranking de confiança de usuários. *Exame*, 24 set. 2020. Disponível em: <https://exame.com/tecnologia/facebook-e-ultimo-colocado-em-ranking-de-confianca-de-usuarios/>. Acesso em: 23 out. 2022.

⁴¹⁴ Um novo recurso que está sendo lançado nesta semana em aparelhos iPhone e iPad, permitindo que usuários rejeitem a coleta de seus dados por aplicativos, vem acirrando a rivalidade entre as gigantes Apple e Facebook. A ferramenta desagradou o Facebook, uma vez que dados de usuários - e os anúncios publicitários embasados neles - são justamente o que tornam a rede social tão lucrativa. Centrado no chamado de IDFA (identificador para anunciantes, na sigla em inglês), o recurso novo implantado pela Apple pode resultar, portanto, em um significativo revés financeiro a esse modelo de negócios. WAKEFIELD, Jane. Apple x Facebook: a nova ferramenta do iPhone que acirra disputa das gigantes da tecnologia. *BBC News. Brasil*. 27 de Abril de 2021. Disponível em: <https://www.bbc.com/portuguese/geral-56905209>. Acesso em 16 de Dezembro de 2022.

⁴¹⁵ “Um novo recurso que está sendo lançado nesta semana em aparelhos iPhone e iPad, permitindo que usuários rejeitem a coleta de seus dados por aplicativos, vem acirrando a rivalidade entre as gigantes Apple e Facebook. A ferramenta desagradou o Facebook, uma vez que dados de usuários – e os anúncios publicitários embasados neles – são justamente o que tornam a rede social tão lucrativa. Centrado no chamado de IDFA (identificador para anunciantes, na sigla em inglês), o recurso novo implantado pela Apple pode resultar, portanto, em um significativo revés financeiro a esse modelo de negócios” (WAKEFIELD, Jane. Apple x Facebook: a nova

que a privacidade dos seus usuários é assunto sério para empresa, passando uma confiança aos seus clientes⁴¹⁶.

Cada vez mais, a confiança na proteção de dados é um diferencial competitivo que as empresas buscam explorar. É até possível afirmar que nasce um novo gênero de consumo identitário, agora ligado a empresas que valorizam a proteção de dados dos seus consumidores. É importante, porém, estar atento a possíveis práticas de *bluwashing* na área de tutela de dados.

Com efeito, entende-se que existe um claro investimento em confiança pelos *players*. A partir do entendimento que a confiança do consumidor nas plataformas é estimulada por esses *players* e que já estamos em uma fase de *hiperconfiança* nas relações de consumo no ciberespaço, faz-se imprescindível um aprimoramento da tutela desse valor no ambiente digital.

Neste sentido, é importante tutelar a confiança dos usuários nas bases de tratamento de dados pessoais, especialmente, do consentimento e do legítimo interesse. Apesar das hipóteses autorizativas garantirem certa segurança jurídica aos titulares, existem assimetrias que dificultam severamente o controle por parte dos usuários, razão pela qual torna-se cada vez mais importante analisar os contratos de tratamento de dados a partir das legítimas expectativas de proteção de dados e de privacidade dos titulares.

Portanto, aborda-se sobre as problemáticas do consentimento e legítimo interesse no ciberespaço, as bases de tratamento mais utilizadas nas relações de consumo na *internet*.

3.1.2 Consentimento viciado: a tônica do ciberespaço

O consentimento foi forjado na segunda geração de leis de dados em função da preocupação da população com a vigilância através dessas informações, desse modo, o titular dos dados vira o protagonista do controle do fluxo informacional, possuindo total responsabilidade⁴¹⁷. A ideia principal na criação desse instrumento de controle foi que o indivíduo tomaria as melhores decisões, buscando otimizar seu bem-estar. Nota-se, a partir desse entendimento, uma roupagem liberal do consentimento, onde acredita-se que o indivíduo sempre decide de maneira favorável a si, buscando melhorar seu bem-estar. Esse pensamento advém da teoria econômica clássica, que considera uma criatura ficcional chamada de *homo*

ferramenta do Iphone que acirra disputa das gigantes da tecnologia. *BBC News Brasil*, 27 abr. 2021. Disponível em: <https://www.bbc.com/portuguese/geral-56905209>. Acesso em: 16 dez. 2022).

⁴¹⁶ ROSA, Bruna. Apple lança primeira campanha sobre privacidade de dados no Brasil e em mais 23 países. *O Globo*, 26 maio 2022. Disponível em: <https://oglobo.globo.com/economia/tecnologia/noticia/2022/05/apple-lanca-primeira-campanha-sobre-privacidade-de-dados-no-brasil-e-em-mais-23-paises.ghtml>. Acesso em: 23 out. de 2022.

⁴¹⁷ BIONI, Bruno. *loc. cit.*, p. 110.

economicus como todos os indivíduos. A premissa central da teoria econômica é que as pessoas escolhem por otimização e que tais escolhas são imparciais⁴¹⁸, assim, os indivíduos tomariam decisões sempre de forma racional.

O consentimento é um instrumento bem conhecido nas leis brasileiras, estando presente em diversas disposições do Código Penal, do Código Civil, assim como encontra-se no MCI e LGPD. Entende-se que o consentimento na matéria de dados possui nítida natureza contratual, havendo uma manifestação de vontade para poder tratar os dados, e do outro lado uma permissão para tal atividade. Cots e Oliveira ressaltam que o consentimento é um negócio jurídico que possui forma prescrita por lei⁴¹⁹.

As legislações sobre proteção de dados elencam requisitos para aferir a validade do consentimento de uma pessoa natural, impondo que esta permissão seja livre, inequívoca e informada. Essa disposição é evidente no artigo 7º do MCI, dispositivo que assegura direitos aos usuários, como o tipificado no art. 7º, VII, da lei 12.965/2014⁴²⁰. Também, o inciso IX, do mesmo artigo infirma a necessidade de o consentimento ser expresso sobre a coleta, uso, armazenamento e tratamento de dados pessoais, inclusive, estando de forma destacada das demais cláusulas contratuais.

A LGPD trouxe uma nova dimensão de proteção das informações pessoais no ciberespaço em solo nacional, trazendo entendimentos novos para tutelar os dados pessoais na *internet*. A legislação traz o conceito de consentimento no seu artigo 5º, inciso XII, ao aludir que o consentimento é a “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”.

Sendo assim, o consentimento é uma das 10 bases de tratamento previstas na LGPD. Neste sentido, é importante ressaltar que não existe hierarquia entre essas bases⁴²¹, devendo o

⁴¹⁸ THALER, Richard. MISBEHAVING: A construção da economia comportamental. Ed. Rio de Janeiro: Intrínseca, 2019. p. 279.

⁴¹⁹ OLIVEIRA, Ricardo; COTS, Marcio. *loc. cit.* p. 91-92.

⁴²⁰ Art. 7º VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, edição 157, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 14 jan. 2022)

⁴²¹ QUINELATO, Pietra. IX Jornada de Direito Civil: esclarecimentos sobre o consentimento. Magis portal jurídico. São Paulo. 1 de Junho de 2022. Disponível em: <https://magis.agej.com.br/ix-jornada-de-direito-civil-esclarecimentos-sobre-o-consentimento/>. Acesso em 13 de Janeiro de 2023.

controlador utilizar-se dos princípios da adequação e necessidade para identificar qual base de tratamento é mais oportuna para aquela situação específica.

Na ocasião do consentimento ser a base de tratamento mais adequada para aquela finalidade, o controlador deverá preocupar-se em garantir que esse aceite seja livre, inequívoco e informado. O conceito de livre aqui se traduz na ideia de que a permissão não seja viciada, isto é, o titular não esteja sob coação ou estado de perigo no momento do aceite, bem como, verificar-se-á a possibilidade de o titular ter incorrido em erro, dolo, simulação ou lesão. Bioni vai além ao afirmar que o adjetivo livre também deve ser entendido como qual o “poder de barganha” entre os atores da negociação, visto que existem relações tão assimétricas que uma das partes é débil na negociação⁴²². Desse modo, para o ordenamento jurídico brasileiro, caso um vício esteja presente, o negócio jurídico pode se tornar anulável, conforme disposição do artigo 171º do Código Civil.

Em relação ao conceito de inequívoco, entende-se que o tratamento de dados deve ser para um propósito específico. Neste sentido, o termo inequívoco possui intrínseca ligação com o princípio da finalidade, desse modo, finalidades genéricas serão incongruentes com a ideia de um consentimento adjetivado⁴²³. É dever da plataforma que busca tratar os dados deixar claro no momento do consentimento qual o objetivo final do tratamento daquelas informações, satisfazendo o princípio da finalidade.

A ideia de informado possui nítida relação com o direito de informação presente no CDC. Compreende-se que todas as condições, finalidades, etapas e procedimentos do consentimento devem ser claras e transparentes ao sujeito natural que está concordando em anuir para o tratamento dessas informações. Sendo assim, é um dever dos *players* informar, dar conhecimento aos riscos e condições do negócio jurídico, nesse caso, do consentimento para o tratamento de dados pessoais.

Com efeito, a informação deve ser ostensiva, contudo, como salienta Miragem informar, não é despejar informações e sim destacar as mais importantes naquele contexto de contratação⁴²⁴. Bioni salienta que a informação garante uma autoproteção ao leigo, ajudando-o a preencher o vazio da assimetria informacional tão patente entre consumidor e plataforma⁴²⁵.

⁴²² BIONI, Bruno. Op. Cit., p. 184.

⁴²³ Ibidem, p. 186.

⁴²⁴ MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. Revista de Direito do Consumidor. Vol 125. 2019. p. 24.

⁴²⁵ BIONI, Bruno. Op. Cit., p. 181.

Desse modo, o consentimento deve ser analisado a partir da sua adjetivação, isto é, será verificado se as condições de ser livre, inequívoco e informado foram cumpridas integralmente pela plataforma sob pena de anulação do negócio jurídico, nesse caso, a revogação do consentimento dado.

Contudo, em que pese os esforços da doutrina em adjetivar o consentimento para garantir uma análise completa, é cediço sua problemática e fragilidade em razão de tamanhas assimetrias presente do ciberespaço⁴²⁶. Neste sentido, o consentimento que sempre teve um papel central na proteção de dados pessoais, sendo o protagonista como o principal instrumento de controle do fluxo informacional do usuário no ambiente virtual está passando por severas crises.

Em função da dependência e dos arranjos dos serviços no ciberespaço, forma de contratação, finalidades genéricas, assimetria informacional, é nítida a impossibilidade de o consentimento servir ao seu propósito, estando quase sempre viciado. O *design* dos serviços da *internet* é criado de uma maneira que ou o consumidor consente com todas as permissões do serviço ou ele não o utilizará. Nessa esteira, Laura Mendes reflete que a opção de não conceder os dados pessoais resultará no impedimento de acesso do indivíduo aos serviços da atualidade⁴²⁷. Somando-se à essa problemática, os serviços tecnológicos assumiram tamanha importância para a vida produtiva na sociedade tecnológica que optar por não os utilizar é uma forma de exílio social, impossibilitando, inclusive, a produção laboral.

Outra questão que impossibilita falar em consentimento adjetivado no atual contexto tecnológico é a forma de contratação. Como sabe-se, os contratos no ciberespaço são os denominados de adesão, sendo assim, o *player* define todas as cláusulas e ao consumidor resta apenas aceitar, no modelo *take it* ou *leave it*. Sendo assim, como falar em consentimento livre?

Além disso, percebe-se que a maioria das solicitações para tratamento de dados são genéricas, limitando-se a famosa frase “utilizamos dados para aprimorar sua experiência”. Com efeito, nota-se baixa adequação dos *players* à LGPD em solo nacional⁴²⁸, sendo raro os *sites*

⁴²⁶ QUINELATO, Pietra. IX Jornada de Direito Civil: esclarecimentos sobre o consentimento. Magis portal jurídico. São Paulo. 1 de Junho de 2022. Disponível em: <https://magis.agej.com.br/ix-jornada-de-direito-civil-esclarecimentos-sobre-o-consentimento/>. Acesso em 13 de Janeiro de 2023.

⁴²⁷ Por outro, também na relação entre privados, é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca de suas informações pessoais. (MENDES, Laura. *A Lei Geral*.... loc. cit., p. 39)

⁴²⁸ CORACCINI, Raphael. *Empresas não conseguem se adaptar à lei de proteção de dados pessoais, aponta pesquisa*. CNN BRASIL. São Paulo. 20 de Agosto de 2021. Disponível em:

que permitem o consentimento granulado. Desse modo, sem o respeito aos princípios da finalidade e adequação é muito difícil falar em consentimento inequívoco conforme a lei preconiza, pois a maioria dos pedidos para tratamento de dados são genéricos.

Agravando esse cenário é clara a assimetria informacional na relação entre consumidor e plataforma. Enquanto a plataforma sabe de informações privilegiadas dos seus usuários, como seus hábitos de consumo e até dados sensíveis, o usuário está vendado dentro da caixa preta dos *players*. Sendo assim, existe uma disparidade de informação entre os atores da negociação, que resulta em uma vulnerabilidade informacional por parte do consumidor.

A tônica do consentimento no ciberespaço é a carência de informação sobre seu procedimento, riscos e finalidade, mas, também, é importante ressaltar que muitos serviços utilizam do que Pasquale denomina de *obsuscation*. Isto é, utilizam-se da abundância de informação como maneira de desinformar, pois muitas informações confundem os indivíduos, desse modo, como falar em consentimento informado?

Em relação aos deveres de informação, importa destacar que para a doutrina consumerista, o direito de informação possui ligação direta com a proteção da confiança do consumidor, garantindo a tutela dos deveres anexos, como de ser transparente na fase pré, de execução e pós contratual. Dessa maneira, a vulnerabilidade informacional decorrente da prática de não prestar informações adequadas e qualificadas é um abuso da confiança do usuário.

Verifica-se, portanto, ser muito difícil falar em consentimento adjetivado no contexto de capitalismo da vigilância. O próprio *design* dos negócios impossibilita a utilização desse instrumento de controle. Dessa maneira, a análise que apenas leva em consideração se houve ou não o consentimento para o tratamento de dados é frágil, sendo insuficiente diante do atual contexto de vigília difusa. Diante dessa problemática é fundamental buscar novas formas de análise sobre a validade dos contratos de consentimento, buscando outros fatores de verificação.

Nessa esteira, entende-se que a teoria da privacidade contextual e o princípio da confiança fornecem as ferramentas para uma análise mais complexa sobre a validade do consentimento e outras bases de tratamento, aferindo o contexto do negócio jurídico, seus impactos sociais e (im)propriedade do fluxo das informações.

A tônica do consentimento no ciberespaço é que essa forma de controle está viciada e grande parte dos consumidores sabem disso. Com efeito, existe uma clara relação entre confiança e consentimento, visto que ao usuário só resta confiar que aquele consentimento, muitas vezes viciado, será minimamente respeitado. Sem poder interferir no contrato, modelo de negócio e nas informações prestadas, o usuário encontra-se hipervulnerável, restando apenas acreditar nas instituições regulatórias e privadas.

3.1.3 A confiança na base de tratamento do legítimo interesse:

A base do legítimo interesse é um ponto em comum entre a legislação brasileira e a GDPR, o diploma comunitário europeu sobre dados pessoais.

O legítimo interesse foi incorporado nos artigos 7º e 10º da legislação brasileira de proteção de dados⁴²⁹. Essa hipótese autorizativa prevê a possibilidade de tratamento de dados conforme a necessidade dos interesses legítimos do controlador ou de terceiros sem a necessidade de consentimento por parte do usuário, exceto quando houver violações de direitos e liberdades fundamentais do titular que exijam proteção de dados⁴³⁰.

Para a utilização dessa base de tratamento é necessário que as situações sejam concretas e com finalidades legítimas. Por situações concretas compreende-se que a utilização do legítimo interesse só será possível diante de uma finalidade específica e caso concreto, não podendo especular situações. Nessa esteira, Oliveira e Cots refletem que o termo “situações concretas” delimita um prazo temporal para o tratamento dos dados pessoais ou impõe urgência no seu enquadramento em base jurídica específica”. Além disso, os autores salientam que as situações concretas são capazes de criar expectativas nas partes, especialmente, no titular⁴³¹, isso significa

⁴²⁹ Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I – apoio e promoção de atividades do controlador; e

II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial

⁴³⁰ AZEVEDO, Ricardo. *loc. cit.*, p. 123.

⁴³¹ OLIVEIRA, Ricardo; COTS, Márcio. O legítimo interesse. In: OLIVEIRA, Ricardo; COTS, Márcio, coordenação. O legítimo interesse e a LGPD. 2. Ed. Ver., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021. p. 77-78.

que o usuário já sabe o que esperar do tratamento de dados, *confiando* que a finalidade do tratamento será respeitada.

Quanto ao termo “finalidades legítimas”, entende-se a “finalidade” definida como a razão específica para o tratamento; em outras palavras, o objetivo do controlador⁴³², enquanto o termo “legítimo” expressa que o interesse deve ser legal, ou seja, que respeite as leis e normas infralegais aplicáveis àquela situação específica⁴³³.

Ressalte-se que essa base de tratamento caracteriza-se pela sua alta carga de discricionariedade, pois o uso dessa hipótese autorizativa não é um direito do titular, mas uma escolha do controlador, que determinará quando realizar o uso da base na relação (enquadramento), assim como poderá escolher a hora de interromper o tratamento dos dados, ressalvado o direito de *opt out* do titular⁴³⁴.

Em função dessa característica do legítimo interesse preconiza-se a realização de uma interpretação sistemática e teleológica do artigo para alcançar o objetivo do diploma. Assim, extrai-se que a base legal é utilizável tanto pelo controlador como pela figura do terceiro⁴³⁵.

Outra sensível lacuna no artigo 10º da LGPD diz respeito às condições de tratamento. Entende-se que, a partir de uma interpretação teleológica, buscando a finalidade do diploma legal, que as condições dos incisos I e II são cumulativas e não alternativas, dessa maneira é necessário que ambos os incisos do artigo sejam satisfeitos. Além disso, o procedimento do controlador deve estar em conformidade com os princípios da LGPD e não violar direitos e liberdades fundamentais do titular, sendo necessário realizar um balanceamento entre os interesses da plataforma e do titular⁴³⁶.

⁴³² BUCHAIN, Luiz Carlos. Proteção de dados: legítimo interesse e consentimento. *Revista da Faculdade de Direito da UFRGS*, Porto Alegre, n. 45, p. 106, 2021. Disponível em: <https://seer.ufrgs.br/revfacdir/article/view/107259>. Acesso em 09 Fev 2023.

⁴³³ BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. *O legítimo interesse na LGPD: quadro geral e exemplos de aplicação*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. p. 20. Disponível em: https://www.researchgate.net/publication/352747913_O_LEGITIMO_INTERESSE_NA_LGPD_QUADRO_GERAL_E_EXEMPLOS_DE_APLICACAO_Associacao_Data_Privacy_Brasil_de_Pesquisa. Acesso em 09 Fev 2023.

⁴³⁴ O exemplo deixa claro que o uso do Legítimo Interesse como base jurídica de tratamento de dados pessoais não é um direito do titular, mas uma discricionariedade do controlador, que poderá, ou fazer o enquadramento, ou interromper o tratamento de dados pessoais por meio de eliminação ou anonimização deles (OLIVEIRA, Ricardo; COTS, Márcio, *O legítimo interesse.. Op. Cit.*, p. 81)

⁴³⁵ Desse modo, por exemplo, extrai-se que a base legal é utilizável tanto pelo controlador como pela figura do terceiro, assim como ocorre na GDPR. Todavia, a diferença é que no diploma europeu essa hipótese está tipificada (VERBICARO, Dennis; CALANDRINI, Jorge. loc. cit., p. 81)

⁴³⁶ BUCHAIN, Luiz Carlos. Op. cit., p. 111.

Pelas características dessa base de tratamento verifica-se que há uma grande preocupação em proteger o titular e suas legítimas expectativas, pois o legítimo interesse notabiliza-se por possuir alta carga de discricionariedade, além de ser utilizada para uso intensivos de dados⁴³⁷, onde há o prolongamento da relação no tempo, o que pode gerar os contratos cativos de longa duração⁴³⁸. Sendo assim, é claro o fator confiança nessa base de tratamento.

Nota-se que o art. 10, II, da LGPD, faz expressa menção às *legítimas expectativas do titular*, notadamente, a palavra-chave quando se refere à confiança nas relações. Revela-se, dessa maneira, uma relação intrínseca entre a confiança do usuário e a base do legítimo interesse, pois o tratamento deve estar em conformidade com as expectativas do titular, ou seja, de acordo com a confiança do consumidor naquele serviço. Dessa maneira, a própria legislação apontou que o tratamento de dados nessa hipótese autorizativa é conforme a confiança do titular. Infirmado esse entendimento, o art. 2º, VI, da LGPD, ao listar os fundamentos da proteção de dados, tipificou a defesa do consumidor, diploma legal que é um verdadeiro microsistema de proteção da confiança do vulnerável. Portanto, mediante uma interpretação teleológica, extrai-se a preocupação do legislador em assegurar a proteção da confiança no art. 10 da LGPD⁴³⁹.

As elucidações de Ricardo Azevedo corroboram com esse entendimento, pois o autor defende que as legítimas expectativas do titular se tornam um contrapeso ao legítimo interesse do controlador, atuando como um limitador⁴⁴⁰. Dessa maneira, o autor desenvolve que a confiança, princípio protegido em diversas leis brasileiras, também, consolida-se na matéria de proteção de dados pessoais a partir da tipificação no art. 10º, II, da LGPD. Sendo assim, o tratamento deve ocorrer para os fins que foram informados ao usuário, analisando objetivamente a correspondência entre a finalidade informada ao titular e aquela efetivamente dada às informações⁴⁴¹.

⁴³⁷ O principal argumento seria que tal hipótese seria mais *flexível* e extremamente pertinente em um cenário de uso intensivo dos dados, já que seria contraproducente e inviável recorrer a todo o momento ao consentimento para legitimar tais tratamentos (BIONI, Bruno. *loc. cit.*, p. 234)

⁴³⁸ VERBICARO, Dennis; CALANDRINI, Jorge. *Op. Cit.*, p. 82 ss

⁴³⁹ *Ibid*, p. 81.

⁴⁴⁰ Assim, o art. 10 e parágrafo 2º, da Lei nº 13.709/2018, estabelece o princípio da confiança, aqui representado pela legítima expectativa do titular do dado, como um verdadeiro contrapeso ao legítimo interesse do controlador dos dados, que somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, observando o princípio da boa-fé (AZEVEDO, Ricardo. *loc. cit.*, p. 118)

⁴⁴¹ Assim, a legítima expectativa do titular dos dados, consubstanciada no Princípio da Confiança, que se encontra em diversos dispositivos da legislação brasileira e agora consolidada especificamente, quanto à proteção de dados, no art. 10 e inciso II, da Lei nº 13.709/2018, deve corresponder aos fins que lhe foram informados e para os quais consentiu com o tratamento de seus dados pessoais, como substituição do conceito subjetivo por uma

A preocupação do legislador mostra-se importante ao atestar-se que as legítimas expectativas do titular são naturais nessa base de tratamento em razão dos seus próprios requisitos: finalidades legítimas e situações concretas⁴⁴². Além disso, em razão da nenhuma ingerência do usuário sobre essa base a proteção da confiança torna-se mais vital.

Sendo assim, em que pese o legítimo interesse ser considerada a base legal de tratamento mais flexível⁴⁴³, ganhando o *status* de versátil entre as demais, sua utilização acarreta um maior ônus argumentativo e probatório do controlador⁴⁴⁴. Verifica-se o ônus probatório do controlador e operador na disposição do artigo 37º da LGPD, que tipifica a obrigatoriedade de ambos em registrar as operações de tratamento de dados pessoais que realizem, especialmente *quando baseado no legítimo interesse*.

Sendo assim, em função da confiança marcante nesse tratamento e sua carga de discricionariedade, há diversas obrigações que o operador/terceiros deve(m) satisfazer para utilizar essa hipótese de tratamento, como o requisito de casos concretos para a aplicabilidade da base legal e o teste de proporcionalidade⁴⁴⁵. Além disso, compreende-se que o estabelecimento de uma relação jurídica prévia para a utilização do legítimo interesse é um importante salvaguarda para o controlador, pois em função da confiança, é razoável que um consumidor espere que uma empresa na qual ele é cliente envie *marketing* dos seus produtos, sendo um legítimo interesse do *player*, que o consumidor legitimamente espera (possui expectativas)⁴⁴⁶.

Além disso, os princípios do artigo 6º da LGPD, possuem incidência horizontal na legislação, aplicando-se as bases de tratamento da lei. Neste sentido, Bioni, Kitayama e Rielli afirmam que “Os princípios também servem como uma barreira de modulação *ao voto de*

análise objetiva da correspondência entre a finalidade informada ao titular e aquela efetivamente dada às informações (*Ibid*, p. 119)

⁴⁴² Duas condições objetivas, geralmente, geram uma expectativa ao titular no contexto de tratamento de dados pessoais: a finalidade do tratamento e a relação jurídica entre controlador e titular (“situações concretas”). (OLIVEIRA, Ricardo; COTS, Márcio. *O legítimo interesse.. loc. cit.*, p. 89)

⁴⁴³ MATTIUZZO, Marcela; PONCE, Paula. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. *Internet & sociedade*, v.1, n.2, p.57, dez. 2020. p. 57. Disponível em: https://www.researchgate.net/publication/359510043_O_legitimo_interesse_e_o_teste_da_proporcionalidade_uma_proposta_interpretativa. Acesso em 09 de Fev 2023.

⁴⁴⁴ BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. *loc. cit.*, p. 30.

⁴⁴⁵ VERBICARO, Dennis; CALANDRINI, Jorge. *loc. cit.*, p. 83.

⁴⁴⁶ Segundo o considerando 47, já mencionado, “poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento”. O texto sugere que um pressuposto para o exercício do Legítimo Interesse poderia ser uma relação jurídica prévia, como poderia ser a de um cliente com o fornecedor ou empregado com o empregador (OLIVEIRA, Ricardo; COTS, Márcio. *O legítimo interesse.. loc. cit.*, p. 106)

confiança dado ao agente de tratamento de dados, que é quem terá discricionariedade para avaliar se o seu interesse é legítimo⁴⁴⁷”.

Com efeito, além do princípio da confiança, os princípios da necessidade e da transparência são fundamentais perante a subjetividade do legítimo interesse. A necessidade (art. 6º, III, LGPD) é garantia de limitação ao tratamento de dados, garantindo que apenas dados necessários sejam tratados. A transparência, princípio de clara relação com a confiança, garantirá um maior controle ao titular sobre o tratamento dos seus dados pessoais, tornando o tratamento mais previsível⁴⁴⁸. Com efeito, a materialização da transparência nessa base de tratamento pode ocorrer, por exemplo, nos procedimentos de aviso de mudanças das Políticas de Privacidade e Tratamento de Dados Pessoais, que mormente, ocorre via e-mail⁴⁴⁹.

Os requisitos e problemáticas que o controlador precisa estar atento para utilizar o legítimo interesse são abundantes. Por outro lado, do ponto de vista do usuário, verifica-se sua total vulnerabilidade na utilização da base do legítimo interesse, não sendo por acaso que criaram a figura do *Legitimate interests assessment (LIA)*, um teste de proporcionalidade para aferir se os requisitos estão sendo cumpridos.

A primeira fase diz respeito à verificação da situação concreta e à finalidade legítima (art. 10, *caput*, e I, da LGPD). Neste sentido, deve-se observar se está presente algum benefício ou vantagem com o uso de dados por parte do controlador, além de averiguar a situação em concreto⁴⁵⁰. A segunda fase diz respeito à necessidade, ou seja, se a base escolhida pelo controlador é a mais adequada no tratamento dos dados e se a quantidade dos dados não é muito intrusiva ao usuário. Dessa maneira, deve-se atentar se os dados coletados são realmente necessários para se atingir a finalidade pretendida⁴⁵¹.

A terceira fase é o balanceamento, onde ocorrerá a aferição dos impactos sobre o titular dos dados e legítimas expectativas (art. 10, II, da LGPD). Para Bruno Bioni, é a principal fase do teste, pois efetivamente sopesam-se os interesses do controlador e titular dos dados. É, justamente, nessa etapa que se verifica a importância da proteção da confiança do usuário na base do legítimo interesse, como uma barreira aos abusos das plataformas. É necessário averiguar se o tratamento dos dados está conforme as legítimas expectativas do titular, ou seja,

⁴⁴⁷ *Ibid*, p. 28. Grifo nosso.

⁴⁴⁸ Quanto ao princípio da Transparência, sua aplicação visa permitir maior controle do titular sobre o tratamento dos seus dados pessoais, que é uma das tônicas da LGPD, bem como tornar o tratamento mais previsível (OLIVEIRA, Ricardo; COTS, Márcio. *O legítimo interesse.. Op. Cit.*, p. 95)

⁴⁴⁹ *Ibid*, p. 96.

⁴⁵⁰ MATTIUZZO, Marcela; PONCE, Paula. *op. cit.*, p. 61.

⁴⁵¹ BIONI, Bruno. *loc. cit.*, p. 237.

se são compatíveis entre o uso adicional e aquele que originou a coleta de dados⁴⁵². Além de atestar nessa fase, se não há violações a direitos e à liberdade fundamentais dos titulares.

Como Bioni já lançou luz, a teoria da privacidade contextual de Helen Nissenbaum, que possui ligação direta com o conceito de expectativas legítimas, oferece o referencial teórico para a aplicação do teste de proporcionalidade, aferindo se a confiança do titular foi respeitada no fluxo das informações, assim como se houve o respeito aos direitos e liberdades fundamentais envolvidos. Neste sentido, compreende-se ser necessário estender a aplicação da teoria devendo ser estendido para as bases de tratamento das relações de consumo, como o consentimento

Como reflete Ricardo Azevedo, a LGPD confirma a ideia de expectativas legítimas do titular para o campo de proteção de dados, sendo um novo imperativo em qualquer base de tratamento analisar o respeito à confiança dos usuários⁴⁵³. Desse modo, compreende-se que o princípio das legítimas expectativas não deve ficar limitado ao legítimo interesse.

Dessa maneira, as legítimas expectativas do titular passam a ser um requisito a ser analisado em toda relação que envolva dados pessoais. Portanto, a proteção da confiança através das legítimas expectativas de proteção de dados garantirá ao titular que os fins informados para o qual consentiu o tratamento foi cumprido, fornecendo uma análise objetiva aos contratos de Tratamento de Dados Pessoais e Políticas de Privacidade.

3.1.4 As legítimas expectativas de privacidade nos contratos de tratamento de dados pessoais no ciberespaço.

Consumir é um ato de confiança, seja a confiança no *branding* ou nas informações prestadas pelo serviço. No atual contexto tecnológico, marcado por dependência do consumidor

⁴⁵² Essa é a principal fase do teste de proporcionalidade na qual efetivamente sopesam-se os interesses do controlador e de terceiros diante dos do titular. Deve-se perquirir: c.1) se o novo uso atribuído ao dado está dentro das *legítimas expectativas* do titular dos dados. Isso é parametrizado pela noção de *compatibilidade* entre o uso adicional e aquele que originou a coleta de dados pessoais. Eles devem ser próximos um do outro, demandando-se uma análise *contextual* para verifica se esse uso secundário seria esperado pelo titular dos dados. Aliás, não foi por outra razão a escolha do termo “legítimo”, o qual qualifica não só a base legal em questão, como, também, o princípio da finalidade; e c.2) de que forma os titulares dos dados serão impactados, especialmente repercussões negativas em termos de discriminação e sobre sua autonomia (*liberdades e direitos fundamentais*). Caso mas não necessariamente, o tratamento de dados também os “beneficie”, a balança tende a estar equilibrada. Em síntese, do início ao fim, essa fase do teste é calibrada pelo vocabulário da teoria da privacidade contextual, devendo-se analisar as legítimas expectativas em jogo, e principalmente, se o fluxo informacional é apropriado-íntegro para o livre desenvolvimento da personalidade do titular (*Ibid*, p. 237)

⁴⁵³ AZEVEDO, Ricardo. *loc. cit.*, p. 135-136.

em serviços da *internet*, o ato de consentir o tratamento de dados também é uma ação de confiança.

Como elucidado, as bases de tratamento do consentimento e do legítimo interesse, as mais usuais nas relações de consumo, são rodeadas por problemáticas e por um vínculo de confiança. É natural que o usuário crie *legítimas expectativas de privacidade e proteção de dados* com o tratamento das informações no qual consentiu ou que está vinculado em razão do legítimo interesse do controlador/terceiro.

A permissão de dados pessoais para tratamento pelas plataformas nada mais é do que um contrato entre consumidor e fornecedor. Desse modo, princípios como a boa-fé e confiança orientam a realização e desenvolvimento dos negócios firmados, pois embora o instituto não esteja no rol de princípios da LGPD, tal fato não diminui sua importância, visto que as bases de tratamento de dados pessoais são contratos, logo, incidirá os princípios do Direito Civil e Direito consumerista⁴⁵⁴. A partir dessa premissa é plenamente possível a aplicação da teoria da confiança para interpretação e análise desses vínculos, protegendo as *legítimas expectativas de privacidade e de proteção de dados*.

É inegável que da realização desses vínculos surgem *legítimas expectativas* por parte dos usuários. O consumidor de um determinado serviço confia nas Políticas de Privacidade e de Tratamento de Dados. Confia que o tratamento de dados solicitados para a finalidade de “aprimoramento do serviço” será utilizado para esse destino e não para compartilhamento com terceiros.

Nissenbaum desenvolve que a privacidade e a tecnologia devem ser compreendidas a partir da vida social dos indivíduos, pois é o social que determina a impropriedade do fluxo das informações ou a incongruência de uma tecnologia com os princípios morais da época de sua criação⁴⁵⁵. Neste sentido, a autora busca responder porque apesar da comunidade global contemporânea viver em uma sociedade confessional, expondo a vida privada cotidianamente na *internet*, existe uma constante preocupação com a erosão da privacidade. Essa dualidade da nossa sociedade pode ser explicada a partir da privacidade contextual, compreendendo que a informação se torna inapropriada dependendo do contexto inserido, das arenas da vida que esses

⁴⁵⁴ Contudo, conforme acenamos, o fato de a boa-fé não ter constado do rol de princípios da LGPD não diminui em nada sua importância. Isso especialmente, porque, como várias bases legais para tratamento de dados pessoais tem fundo contratual, com destaque para o consentimento, a boa-fé poderá incidir seus efeitos também como princípio, pois se trata de princípio contratual reconhecido pelo Direito Civil (OLIVEIRA, Ricardo; COATS, Marcio. *loc. cit.*, p. 78)

⁴⁵⁵ NISSENBAUM, Helen. *Privacy in context. loc. cit.*, p. 4-11.

dados invadem⁴⁵⁶.

Para a autora, a informação possui um valor social, desse modo, a integridade do tráfego dos dados pessoais deve respeitar um contexto de uma relação; em outras palavras, a privacidade deve ser pensada conforme uma integridade contextual. Para Nissenbaum, as informações pessoais podem ser apropriadas ou não dependendo do local e do contexto na qual esses dados estão sendo revelados, devendo sempre realizar uma análise contextual de cada caso⁴⁵⁷. Dessa forma, as informações que não possuem nenhuma conexão com o contexto da relação não respeitam a integridade do fluxo informacional, como, em uma dinâmica de trabalho, um indivíduo falar sobre a religião ou orientação sexual de um colega de emprego, sendo tal revelação inapropriada para o contexto do diálogo⁴⁵⁸.

A teoria da privacidade contextual entende que existem várias esferas de informações que circulam os indivíduos nos mais variados locais da vida cotidiana. Assim, há diversos reinos que os indivíduos fazem parte, os quais possuem suas próprias normas sociais. Assim, para Nissenbaum, há dois tipos de normas informacionais: normas de adequação e normas de distribuição. Para a autora “A integridade contextual é mantida quando ambos os tipos de normas são mantidos, e é violada quando qualquer uma das normas é violada⁴⁵⁹”.

Nissenbaum sustenta que a norma de adequação (*appropriateness*) diz respeito a qual informação pessoal é apropriada para ser revelada em determinado contexto, ou seja, são normas que versam sobre a natureza da informação. Ao explicar esse ponto, Nissenbaum utiliza o exemplo médico e paciente, onde é totalmente apropriado dividir detalhes da saúde (dados sensíveis) ao médico, mas, provavelmente, isso em outro contexto não seja apropriado, enquanto as normas de distribuição (*distribution*) são aquelas que avaliam o fluxo de informações ou de transferência da informação para um terceiro, aferindo se foram de acordo com as expectativas do titular⁴⁶⁰. Logo, se o tratamento de uma plataforma é para produção de

⁴⁵⁶ Between the ground and the heavens, according to the picture I am imagining, is the real of the social, and it is in this real that contextual integrity fits. This middle real holds a key to explaining why people react to real world disputes in the ways they do and why they frequently express their alarm in terms of the erosion of privacy (*Ibid*, p. 11)

⁴⁵⁷ Um princípio central da integridade contextual é que não há arenas da vida não regido por *normas de fluxo de informações*, nenhuma informação ou esferas de vida para a qual ‘vale tudo’. Quase todas – as coisas que fazemos, eventos que ocorrem, transações realizadas – acontecem em um contexto não apenas de lugar, mas de política, convenção e expectativa cultural (NISSENBAUM, Helen. *loc. cit.*, p. 137, tradução nossa – destaque do original)

⁴⁵⁸ VERBICARO, Dennis; CALANDRINI, Jorge. *loc. cit.*, p. 86.

⁴⁵⁹ *Contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated* (NISSENBAUM, Helen.. *op. cit.*, p. 138)

⁴⁶⁰ *Ibid*, p. 138-140.

conteúdo, como no exemplo da corretora utilizado no trabalho, não faz parte do contexto a empresa coletar dados sensíveis, que não possuem ligação com o início da relação.

Desse modo, Nissenbaum elucida que “O que importa é não apenas se as informações são apropriadas ou inadequadas para um dado contexto, mas se sua distribuição, ou fluxo, respeita normas contextuais de fluxo de informações”⁴⁶¹. Portanto, o foco é analisar como a dinâmica do tráfego informacional está em conformidade com a relação que lhe dá origem – a causa primária da coleta e o tratamento de dados –, bem como se o compartilhamento daquela informação respeita a expectativa do titular.

Bruno Bioni, ao falar sobre o trabalho de Nissenbaum, divide em fluxo interno e externo. O que é similar aos conceitos das normas de adequação e distribuição⁴⁶². Dessa maneira, para Bioni, a análise contextual permite aferir se a informação utilizada possui adequação com a relação inicial e, posteriormente, se o eventual compartilhamento desses dados respeita as legítimas expectativas do titular das informações⁴⁶³. Logo, para Bruno Bioni, o fluxo interno diz respeito à conexão estabelecida entre o emissário e o recipiente da informação – como no exemplo médico e paciente –, enquanto o fluxo externo versa sobre a transferência dessa informação a terceiros.

Bioni esclarece que “Ao final, cada contexto exprime as expectativas de privacidade que o titular das informações deposita, na condição de emissor, no recipiente, e de como esse fluxo informacional fluirá interna e externamente⁴⁶⁴”. Desse modo, a teoria considera que cada contexto cria suas próprias legítimas expectativas de privacidade de como as informações irão fluir⁴⁶⁵, percebendo-se assim, a nítida relação da teoria com a proteção das legítimas expectativas do titular, garantindo que a fidelidade depositada pelo emissor (consumidor) aos recipientes (plataforma) seja conforme sua confiança, que o contexto de uma relação já preestabelecida não trairá sua capacidade de autodeterminação informativa e participação

⁴⁶¹ *Ibid*, p. 141.

⁴⁶²: A partir dessa abordagem, será possível não só investigar a operação inicial da coleta e processamento dos dados – momento em que se dá a troca (trade off) dos dados pessoais para se acessar um produto ou serviço (fluxo interno) – mas, também, o compartilhamento desses dados com terceiros (fluxo externo) (BIONI, Bruno. *loc. cit.*, p. 199)

⁴⁶³ *Ibid*, p. 199.

⁴⁶⁴ *Ibid*, p. 201.

⁴⁶⁵ O saldo final da teoria (equação) da privacidade contextual consiste, portanto, na consideração de que em cada contexto o titular dos dados pessoais tem legítimas expectativas (de privacidade) de como eles irão fluir de forma apropriada. O tráfego dos dados pessoais não se dá, portanto, no vácuo, mas sob um conjunto de circunstâncias que determinam a sua integridade (*Ibid*, p. 201)

social⁴⁶⁶.

Com a consolidação do conceito de legítimas expectativas na LGPD⁴⁶⁷ a proteção da confiança torna-se um imperativo. As legítimas expectativas estão diretamente ligadas ao princípio da finalidade e autodeterminação informativa, assim como, sua aferição dependerá de uma análise contextual, aferindo a (in)conformidade do fluxo das informações que estão sendo reveladas. Com efeito, a teoria da privacidade contextual revela-se, mais uma vez, fundamental para a proteção da confiança do usuário na proteção de dados.

Portanto, quando um indivíduo revela uma informação pessoal em determinado contexto ele confia no receptor, criando legítimas expectativas. Essa confiança, também, refere-se a como esse receptor irá distribuir a informação, ou seja, em que pese a confiança dada para revelar um dado pessoal, essa *fides* não garante ao receptor distribuir a informação como quiser.

Sendo assim, o usuário confia que a finalidade na qual o dado foi permitido será respeitada pelas plataformas, mesmo que todo o sistema de tratamento dessas informações seja uma caixa preta. A confiança no tratamento de dados é patente ao se levar em consideração que apenas as empresas sabem como esse procedimento ocorre, sendo práticas totalmente obscuras aos usuários comuns. Quando não há *accountability* e apenas obscuridade, restam as instituições e as pessoas apenas confiar que tudo está sendo realizado conforme apresentado.

Todavia, conforme demonstrado, o ciberespaço é um ambiente que abusa reiteradamente da confiança dos usuários, sendo normal o compartilhamento de dados pessoais à terceiros não envolvidos na relação. Na maioria das vezes o abuso de confiança ocorre na fase de formalização do contrato de adesão no ciberespaço, já autorizando compartilhamentos escusos à margem das legislações de dados, pois poucos são os consumidores que leem os termos de serviços dos aplicativos que utilizam, e os poucos que leem possuem dificuldades em entender suas cláusulas.

Segundo a OIT, ao realizar um relatório sobre as condições dos trabalhadores no capitalismo de plataforma, poucos usuários leem e entendem os termos de serviço e privacidade dos *players*⁴⁶⁸. Como salientam os autores, um dos motivos para o pouco entendimento desses

⁴⁶⁶A privacidade contextual reside justamente na fidelidade depositada pelo emissor de uma informação ao(s) seu(s) recipiente(s), na legítima expectativa de que seus dados pessoais serão usados e compartilhados de acordo com o contexto de uma relação preestabelecida ou a razão pela qual foi publicizado um dado, particularmente, na esperança de que o trânsito das suas informações pessoais não minará e trairá sua capacidade de livre desenvolvimento da personalidade e participação social (*Ibid*, p. 229)

⁴⁶⁷ AZEVEDO, Ricardo. *loc. cit.*, p. 119.

⁴⁶⁸ However, many workers in the app-based taxi (58 per cent) and delivery (49 per cent) sectors reported that they had not seen their platform's terms and conditions. Of those who had seen the terms of service agreements

termos é em razão da linguagem tecnicista, com informações abundantes e muitas sem importância⁴⁶⁹. Ainda em relação aos termos de serviços, é importante ressaltar que não há autonomia de negociação, pois caso o consumidor discorde de algum item do documento, este estará fadado a não utilizar o serviço, visto não ser possível haver negociação em relação à essas cláusulas.

Sendo assim, é evidente que o consumidor é obrigado a confiar nas plataformas, suas Políticas de Privacidade e seus métodos. Em decorrência dessa *fides*, é natural o nascimento de legítimas expectativas de privacidade dos usuários. Se a plataforma informa que os dados coletados são para fins estatísticos e de personalização do serviço, é natural que o consumidor possua expectativas que seus dados serão usados única e exclusivamente para essas finalidades. Contudo, o que se percebe é o abuso da confiança dos consumidores pelas plataformas. Bioni analisa alguns casos polêmicos de termos de serviços que elucidam o abuso da confiança dos usuários pelos *players*.

O *Google*, em 2012, consolidou as 70 (setenta) políticas de privacidade de todos os seus serviços em um único termo com a justificativa de “melhorar a experiência” dos usuários. Todavia, a mudança foi mal-recebida pelo mercado, pois possibilitava a agregação desproporcional de informações pessoais pela empresa dominante do setor⁴⁷⁰. O *Facebook*, ao lançar o aplicativo *Messenger*, em 2014, também buscou utilizar da confiança dos usuários para conseguir maior interferência nas informações pessoais ao lançar uma política de privacidade para o App permitindo, por exemplo, a leitura das mensagens enviadas pelos usuários⁴⁷¹. Nessa mesma esteira, a Samsung *Smart Tv*, em 2015, lançou no seu termo de privacidade que a empresa poderia coletar informações através do microfone do televisor, que poderiam ser compartilhadas com terceiros⁴⁷².

Atualmente, a rede social *TikTok*, sofre severas críticas pelos seus termos de privacidade. Pesquisadores alertam que a política de privacidade aceita pelos usuários para

applicable to them, almost one third reported not having read, not remembering or not having understood them. (ILO. *loc. cit.*, p. 182)

⁴⁶⁹ VERBICARO, Dennis; VIEIRA, Janaína. *loc. cit.*, p. 203.

⁴⁷⁰ BIONI, Bruno. *loc. cit.*, p. 217.

⁴⁷¹ De acordo com os termos dessa nova política de privacidade, o novo aplicativo poderia ler e editar mensagens de texto, gravar áudio e vídeos, fazer ligações e tirar fotos, sendo que em todas essas ocasiões não haveria a necessidade de (“nova”) autorização (intervenção ou confirmação) do usuário para tais práticas (*Ibid*, p. 219)

⁴⁷² *Ibid*, p. 219-220.

utilizar a rede social permite, inclusive que a empresa monitore as teclas digitadas, sabendo o que o usuário está digitando⁴⁷³.

Verifica-se pelos casos apresentados que as empresas buscam, através da confiança em seus serviços, abusar de direitos fundamentais com seus termos de serviço e Políticas de Privacidade. Agravando essa situação, nota-se que o consentimento, teoricamente criado para garantir um controle das informações, já foi totalmente esvaziado pelos *players*. Em função dessa situação, não é mais possível analisar se o tratamento de dados por uma plataforma foi lícito apenas aferindo se houve ou não o consentimento, sendo vital aprimorar o conceito de legítimas expectativas na proteção de dados.

Como demonstrado, o instrumento central de controle do fluxo de informações por parte do titular foi minado com a instituição do capitalismo da vigilância, desse modo, o consentimento mostra-se incapaz de satisfazer o seu propósito. Na presente conjuntura, o consumidor só utilizará o serviço de um *player* se consentir com o contrato padronizado de tratamento de dados da plataforma, sem nenhuma possibilidade de negociar seus direitos fundamentais. Desse modo, os consumidores dependentes dos serviços tecnológicos para exercerem os atos da vida moderna, consentem com Políticas de Privacidade e de Proteção de Dados totalmente à margem das legislações de dados.

Além de toda a problemática do consentimento verifica-se que o legítimo interesse, base que ganha relevância a cada ano, está rodeado de subjetividade que agravam a vulnerabilidade do titular dos dados. Como analisado, o enquadramento dessa base de tratamento é faculdade do controlador ou terceiro, não sendo um direito do titular, ressalvada a salvaguarda do *opt out* do titular. Além disso, o legítimo interesse caracteriza-se por ser uma hipótese autorizativa com alta carga de confiança entre titular e controlador/terceiro. Nota-se essa característica pela sua própria finalidade, que é a utilização para uso contínuo e intensivos de dados, ou seja, é uma relação que se prolonga no tempo, provocando ainda mais necessidade de confiança na relação contratual.

Observa-se que o usuário é compelido a confiar nas plataformas, seus contratos e formas de tratamento, mesmo que sejam caixas-pretas. Desse modo, é natural que o usuário crie legítimas expectativas sobre aquela relação jurídica, esperando legitimamente que a plataforma

⁴⁷³ NIEVA, Ricardo. Navegador no aplicativo do TikTok inclui código que pode monitorar suas teclas digitadas, diz pesquisador. FORBES. Estados Unidos. 18 de Agosto de 2022. Disponível em: <https://www.forbes.com/sites/richardnieva/2022/08/18/tiktok-in-app-browser-research/?sh=3e5ccabc7c55>. Acesso em 12 de Janeiro de 2023.

tratará os dados conforme a finalidade requerida e que estará protegido contra vazamento das suas informações pessoais.

Com efeito, a partir da concretização do conceito de legítimas expectativas na matéria de dados no Brasil, torna-se vital um aprimoramento do conceito e sua aplicação. Em relação ao aprimoramento do conceito para o campo de proteção de dados, entende-se existir farta base teórico para o seu aperfeiçoamento através da tutela da confiança nas relações negociais, utilizando-se do diálogo de fontes com o Código Civil e CDC. No que tange a forma de aplicação do conceito entende-se que a teoria da privacidade contextual pode ser a bússola que norteará a aplicação das legítimas expectativas do titular, realizando uma análise contextual, aferindo o respeito aos princípios da finalidade, confiança e autodeterminação informativa.

Desse modo, entende-se que a confiança e a boa-fé são veículos para a aplicação do conceito de legítimas expectativas do titular e da privacidade contextual no campo de proteção de dados pessoais em solo brasileiro⁴⁷⁴, garantindo o respeito às legítimas expectativas de privacidade dos titulares.

3.2 A responsabilização civil pela frustração das legítimas expectativas de privacidade do consumidor nos casos de vazamentos de dados e de desvio de finalidade do tratamento de dados.

É inegável a incidência do princípio da confiança nos contratos eletrônicos, sendo fundamental o aprimoramento da sua tutela no ciberespaço. Neste sentido, identifica-se que a confiança incide em cada uma das fases do contrato eletrônico, desde o momento pré-contratual até a etapa pós-contratual. Durante esse *iter contratual*, se houver expectativas legítimas frustradas, haverá um dever de responsabilização.

Como ensina Larenz, a proteção da confiança é fonte autônoma de responsabilidade⁴⁷⁵, sendo assim, considerando que para os *players* é vantajoso causar danos no mercado de

⁴⁷⁴ VERBICARO, Dennis; CALANDRINI, Jorge. *loc. cit.*, p. 88.

⁴⁷⁵ SCHMIDT, André Perin. *loc. cit.*, [e-book, cap. 3]: De acordo com o renomado jurista Karl Larenz, esse princípio (Vertrauensprinzip) é ingênito a toda a ciência do Direito, e sua proteção (Vertrauensschutz) "é fonte autônoma (Vertrauensstatbestand) de responsabilidade (Vertrauenshaftung)". Conforme esse doutrinador, quando alguém age, espera pelas consequências de seu ato, e para que alcance o resultado esperado deve poder confiar na conduta dos demais e nas condições criadas por estes. Larenz dá uma dimensão social – no sentido do indivíduo perante a sociedade – a esse princípio ao relacioná-lo com o princípio da responsabilidade (Verantwortungsprinzip). Ao garantir que os indivíduos livres e sociais (Selbstbestimmung) responderão pelos seus atos (Selbstverantwortung) e respeitarão a dignidade alheia (Achtung der Personwürde), cria-se a harmonia nas relações jurídicas, o que é a finalidade da confiança. É

consumo, é fundamental enfrentar essas práticas abusivas, que ocorrerá através da responsabilização das plataformas em razão das legítimas expectativas de privacidade frustradas.

Como elucida Guilherme Martins “O mandamento da proteção da confiança está intimamente ligado ao anonimato das novas relações sociais e à massificação das relações contratuais e pré-contratuais, da produção e comercialização, por vezes sem a possibilidade de se identificar claramente os consumidores e usuários⁴⁷⁶”, como ocorre no ciberespaço. Nessa esteira, entende-se que na contratação no ciberespaço, a confiança dos contratantes deve ser tutelada em face da especificidade do meio, garantindo uma expectativa legítima da parte sob o ponto de vista da segurança e informação. Dessa maneira, a confiança deve funcionar como o parâmetro para a distribuição dos novos riscos trazidos pela comodidade e facilidade decorrentes da evolução tecnológica⁴⁷⁷.

Os maiores temores e riscos presentes para os usuários na atualidade são os advindo da segurança dos serviços e em relação à observância das disposições sobre legislações. Neste sentido, Cots e Oliveira salientam que a boa-fé deverá ser a premissa na interpretação dos contratos de tratamento de dados e, que se excedidos os seus limites, será possível pleitear responsabilização em razão do ato ilícito conforme o artigo 187º do Código Civil⁴⁷⁸.

Desse modo, defende-se que o instituto da responsabilidade civil apresenta-se como a via que garantirá a reparação dos *danos* causados em razão de frustração das legítimas expectativas. Com a mudança de abordagem da responsabilidade civil, o instituto possui o objetivo de reparar os prejuízos de quem sofreu o dano, sendo assim, adota-se a teoria do risco, desvinculando a responsabilidade da voluntariedade do ato⁴⁷⁹.

Em relação à responsabilidade civil na matéria de dados compreende-se que a LGPD, no seu artigo 42º, definiu a responsabilidade objetiva dos agentes de tratamento

graças à confiança que nos movimentamos em busca de uma relação com os demais. O próprio termo "negócio", etimologicamente, significa não ócio, do latim nec + otium, isto é, negociar é agir.

⁴⁷⁶ MARTINS, Guilherme M. Confiança e aparência nos contratos eletrônicos de consumo via internet. *Doutrinas Essenciais de Responsabilidade Civil*. São Paulo: Ed. RT.. Vol. 8. p. 1311-1342. Out. 2011. p. 1311.

⁴⁷⁷ *Ibid*, p. 1312.

⁴⁷⁸ As disposições citadas anteriormente são muito reveladores, pois, de um lado, a boa-fé deve ser premissa na interpretação dos negócios jurídicos e, de outro lado, orientará as partes em todas as fases de formação e execução do contrato. Tão grande é a relevância da boa-fé nas relações jurídicas que, se excedido os seus limites, poderá ser caracterizado ato ilícito passivo de condenação e indenização ao prejudicado (OLIVEIRA, Ricardo; COATS, Marcio. *loc. cit.*, p. 78)

⁴⁷⁹ MARTINS, Guilherme M; LONGHI, João Victor R. Responsabilidade Civil na Lei Geral de Proteção de Dados, Consumo e a Intensificação da Proteção da Pessoa Humana na Internet. *Revista de Direito do Consumidor*. Vol. 139. p. 101-124. Jan- Fev. 2022. p. 101.

(controlador/operador), tendo em vista o risco da atividade⁴⁸⁰. Como critica Martins, a afirmação que a LGPD pode gerar responsabilidade subjetiva é um retrocesso, pois como explica, o regime subjetivo criou injustiças no passado ao fazer que todos os danos recaíssem sobre as vítimas. Na defesa da modalidade objetiva na LGPD, Martins reflete que a crítica relacionada a possibilidade de ampliar as demandas ressarcitórias e inibir o desenvolvimento tecnológico não deve prosperar pois a história demonstrou que a objetivação da responsabilidade em nada obistou a evolução tecnológica⁴⁸¹.

Dessa forma, como ensina Claudia Lima Marques a noção de culpa e presunção de negligência/imperícia não são suficientes para dividir de forma justa os novos riscos da sociedade de consumo⁴⁸². Portanto, a LGPD seguiu o CDC na modalidade de responsabilidade adotada, infirmando ainda mais o diálogo entre essas fontes.

É pacífico que o CDC adota a modalidade objetiva da responsabilidade, não sendo necessário demonstrar culpa do agente infrator, inteligência que se extrai do artigo 12 e 14 do diploma consumerista. Contudo, Martins salienta que a grande diferença entre os regimes adotados nos dois diplomas é a amplitude da solidariedade, pois enquanto a LGPD reconheceu a solidariedade entre operador e controlador no art. 42º, § 1º, o CDC tipifica a solidariedade como regra⁴⁸³.

Dessa maneira, filiando-se ao posicionamento de Martins, entende-se que os danos decorrentes dos incidentes de segurança, como vazamentos não intencionais e invasão de sistemas e bases de dados por terceiros não autorizados, devem ser situados como riscos intrínsecos à atividade de tratamento de dados, sendo necessária a responsabilização dos

⁴⁸⁰ Numa interpretação sistemática do artigo 42, deve ser afirmada como regra geral na Lei Geral de Proteção de Dados a responsabilidade objetiva dos agentes de tratamento, ou seja, o controlador e o operador, tendo em vista o risco da atividade. Tal conclusão decorre do artigo 927, parágrafo único, do Código Civil (LGL\2002\400), em cujos termos haverá obrigação de indenizar o dano, independentemente de culpa, nos casos especificados em lei, ou, como é a hipótese da proteção de dados pessoais, quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. Tal norma se aplica aos danos ocorridos em qualquer fase do processamento de dados pessoais (*Ibid*, p. 104)

⁴⁸¹ MARTINS, Guilherme M; LONGHI, João Victor R. *op. cit.*, p. 105.

⁴⁸² MARQUES, Claudia Lima. *Contratos.. loc. cit.* p. 1345.

⁴⁸³ A diferença mais importante entre os regimes da LGPD e do CDC (LGL\1990\40) está na amplitude das hipóteses de responsabilidade solidária. Enquanto na LGPD o reconhecimento da responsabilidade solidária se submete ao artigo 42, § 1º 41, a responsabilidade nas relações de consumo, em regra, é solidária (Lei 8.078/1990 (LGL\1990\40), artigo 7º, parágrafo único, combinado com artigo 25, §§ 1º e 2º), facilitando a reparação do dano sofrido pelo consumidor (MARTINS, Guilherme; LONGHI, João Victor. *op. cit.*, p. 107)

agentes de tratamento em virtude de tais fatos⁴⁸⁴. Bem como, compreende-se que o desvio de finalidade no tratamento de dados por parte do *player* deve ensejar a responsabilização.

O dever de responsabilização tem como base legal os artigos 187º e 927º do Código Civil e artigo 42, caput, da LGPD. O fundamento para a responsabilização nos casos citados é a frustração das legítimas expectativas do titular. No caso de vazamento, das legítimas expectativas de segurança frustradas. Na situação do desvio de finalidade, em razão das legítimas expectativas de observância das legislações por parte das plataformas.

Em relação à responsabilidade pelo desvio de finalidade do tratamento, entende-se que a hipótese de responsabilização está presente nos artigos 44º, caput e 42º, § 1º da LGPD, em razão do descumprimento das disposições legislações constantes na LGPD. O artigo 44º dispõe que “O tratamento de dados pessoais será irregular *quando deixar de observar a legislação* ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes”. Enquanto o 42º, § 1º, I, da LGPD tipifica que “o operador responde solidariamente pelos danos causados *pelo tratamento quando descumprir as obrigações da legislação de proteção de dados* ou quando não tiver seguido as instruções lícitas do controlador”.

Sendo assim, compreende-se que o dever de indenizar resulta da violação das legítimas expectativas do titular com o tratamento. Salienta-se que nesse caso o consumidor poderá demandar perante o controlador e operador em razão da solidariedade instituída no artigo⁴⁸⁵. Para essas situações, a LGPD, no seu artigo 42, § 2º, estabeleceu a inversão do ônus da prova em favor dos títulos, em um claro diálogo com o art. 6º, VIII, do CDC⁴⁸⁶

No que tange a responsabilização por vazamento de dados, defende-se que o artigo 44º, inspirado nas lições consumeristas, propicia essa possibilidade. O artigo em comento dispõe que “o tratamento de dados será irregular quando não fornecer a segurança que *o titular dele*

⁴⁸⁴Os danos decorrentes dos incidentes de segurança que se relacionam ao risco inerente ao desenvolvimento de atividade de tratamento de dados, como vazamentos não intencionais e invasão de sistemas e bases de dados por terceiros não autorizados, devem ser situados como riscos intrínsecos à atividade de tratamento de dados, e considerados como fortuito interno, não podendo ser afastada a obrigação de indenizar dos agentes de tratamento em virtude de tais fatos (*Ibid*, p. 105)

⁴⁸⁵ Os dois incisos do § 1º do artigo 42 da LGPD, de forma semelhante do RGPD europeu, estabelecem as hipóteses expressas em que haverá solidariedade entre operadores e controladores de dados. No primeiro caso, tem-se a responsabilidade civil solidária por danos causados pelo tratamento que descumprir as obrigações da legislação de proteção de dados ou que não seguir as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador. No segundo caso, tem-se a solidariedade dos controladores que estiverem diretamente envolvidos no tratamento, quando forem vários (*Ibid*, p. 106)

⁴⁸⁶ Por seu turno, o § 2º do art. 42 da LGPD estabelece uma inversão do ônus da prova em favor do titular de dados pessoais, dialogando com o artigo 6º, VIII, da Lei 8.078/1990 (LGL\1990\40), mesmo quando não houver relação de consumo (*Ibid*, p. 106)

pode esperar. Na disposição do artigo é possível notar a incidência do conceito de legítimas expectativas ao tipificar o termo “que o titular dele *pode esperar*”. Dessa forma, é claro que o consumidor espera, legitimamente, que as plataformas fornecerão segurança em relação aos seus dados pessoais. Tal confiança é frustrada quando existem vazamento dessas informações por debilidade dos sistemas de proteção dos *players*.

Neste sentido, compreende-se que a disposição do artigo 44 da LGPD em conjunto com o conceito de legítimas expectativas do titular garantem a responsabilização das plataformas em caso de vazamento de informação, garantido a confiança que o consumidor depositou na segurança do serviço do *player*.

Portanto, a proteção da confiança do consumidor pode ser realizada em uma dimensão negativa, através da responsabilização das plataformas em razão dos seus atos ilícitos. Neste sentido, a frustração das legítimas expectativas do titular torna-se fundamento para a responsabilização. Como exemplo dessas possibilidades, entende-se que nos casos de desvio de finalidade do tratamento e vazamento de dados, a aplicação da teoria da confiança na responsabilidade civil é plenamente possível, possuindo base legal tanto na LGPD como no CDC.

Todavia, a responsabilização civil dessa forma apresenta-se apenas como um meio individual de resolução de conflitos, enquanto os danos na *internet* são coletivos. Dessa forma, é vital falar sobre tutela coletiva na matéria de proteção de dados, buscando incentivar mudanças estruturais.

3.2.1 A tutela coletiva como instrumento de responsabilização das plataformas

Consumir, é na maioria das vezes um ato individual, mas os efeitos das relações de consumo são coletivos. Quando um consumidor tem seu direito violado, quase sempre, outros consumidores também tiveram direitos infringidos. Freddie Didier e Hermes Zaneti, entendem que os processos coletivos servem à “litigação de interesse público”⁴⁸⁷. Para os autores “servem às demandas judiciais que envolvam, para além dos interesses meramente individuais, aqueles

⁴⁸⁷ DIDIER, Fredie JR; ZANETI, Hermes JR. *Curso de Direito Processual Civil: Processo coletivo*. Bahia. Editora JusPODIVIM. 9ª Edição, 2014. p. 33.

referentes à preservação da harmonia e à realização dos objetivos constitucionais da sociedade e da comunidade”⁴⁸⁸.

Com a tipificação da defesa do consumidor no artigo 5º, inciso XXXII, da Constituição Federal, nota-se os consumidores como uma parcela da comunidade constitucionalmente reconhecida e, que a defesa desse grupo é um objetivo da Constituição cidadã⁴⁸⁹. Sendo assim, a defesa dos consumidores constitui um interesse coletivo primário, isto é, um conjunto de interesses coletivos prevalente na sociedade⁴⁹⁰.

No Brasil, a tutela coletiva é cabível nas relações consumeristas, conforme o artigo 1º, II, da lei nº 7.347/85 (LACP). O instituto da tutela coletiva possui amplo alcance no ordenamento pátrio, admitindo-se provimentos jurisdicionais, condenatórios, constitutivos, declaratórios, executivos lato sensu e mandamentais. Ressalta-se que a tutela coletiva admite a inversão do ônus financeiro da prova ao demandando, um importante e necessária medida para a defesa do vulnerável nesses casos. Quanto aos seus efeitos, percebe-se um sistema híbrido no âmbito dos direitos individuais homogêneos, pois o indivíduo do grupo pode optar em continuar na ação coletiva (*right to opt in*) ou escapar dos efeitos da decisão da ação coletiva (*right to opt out*)⁴⁹¹.

Ao falar sobre o conceito de demandas coletivas, Freddie Didier e Zaneti Jr, entendem que a definição deve englobar a ideia de interesse primário. Assim, os autores aludem que “a ação coletiva precisa caracterizar-se como um processo de interesse público⁴⁹²”. Nesta esteira, os processualistas ressaltam que, embora haja alguma resistência quanto à presença constante de interesse público, “o elevado número de pessoas e características da lesão sempre indicam a constância do interesse público primário nos processos coletivos. Daí a obrigatoria e constitucional intervenção do Ministério Público nas demandas coletivas⁴⁹³”.

Percebe-se, desta maneira, como as demandas coletivas podem ser instrumento para mudanças estruturais. É comum em demandas coletivas que estejam presentes mais de um tipo de direitos coletivos, sendo importante identificá-los. O CDC, estipulou no seu artigo 81º,

⁴⁸⁸ *Ibid*, p. 33.

⁴⁸⁹ *Ibid*, p. 33.

⁴⁹⁰ *Ibid*, p. 34.

⁴⁹¹ VERBICARO, Dennis. Resgatando a importância da transação coletiva de consumo no Brasil. *Revista Jurídica UNICURITIBA*. Vol. 03, nº. 48. Curitiba. 2017. p. 94-117. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produto_s/bibli_informativo/bibli_inf_2006/Rev-Juridica_UNICURITIBA_n.48.05.pdf . Acesso em 23 Jun de 2021. p. 98-99.

⁴⁹² DIDIER, Fredie JR; ZANETI, Hermes JR. *loc. cit.*, p. 34.

⁴⁹³ *Ibid.*, p. 38.

parágrafo único, incisos I, II e III os conceitos de direitos difusos, coletivos stricto sensu e individuais homogêneos. Entende-se os direitos difusos como aqueles transindividuais (metaindividuais, supraindividuais), que pertencem à uma coletividade, formando um todo indivisível. Esse conjunto de indivíduos está ligado por circunstâncias fáticas, não havendo uma relação jurídica base entre eles, como por exemplo, na veiculação de publicidade enganosa ou abusiva através do ciberespaço, afetando um número incalculável de consumidores⁴⁹⁴.

Os direitos coletivos em sentido estrito, também são caracterizados pela indivisibilidade. Todavia, a sua diferença em comparação com os direitos difuso reside na relação jurídica prévia⁴⁹⁵. Os direitos individuais homogêneos são divisíveis e possuem como objetivo garantir proteção coletiva aos indivíduos que foram afetados. Esses direitos têm sua origem nas *class actions for damages*, que são ações de reparações de danos à coletividade. Sobre essa categoria, Freddie Didier e Hermes Zaneti Jr, afirmam que são “os direitos nascidos em consequência da própria lesão, ou, mais raramente, ameaça de lesão, em que a relação jurídica entre as partes é *post factum* (fato lesivo)⁴⁹⁶”.

Como elucida Roque “a categorização de um direito coletivo, portanto, dependerá invariavelmente da análise da causa de pedir e do pedido de tutela jurisdicional concretamente formulado⁴⁹⁷”. Desse modo, nos casos que envolvam a tutela de dados, é possível vislumbrar a incidência de todos os tipos de direitos coletivos, dependendo da análise do caso concreto.

A LGPD, em seu artigo 22º, confirma a possibilidade da defesa dos interesses e direitos dos titulares ser pela via coletiva, deixando clara a possibilidade da tutela coletiva na matéria de proteção de dados pessoais. Assim como, o artigo 42, § 3º, prevê que as ações de reparação por danos coletivos que tenham por objeto a responsabilização dos agentes de tratamento podem ser exercidas coletivamente em juízo⁴⁹⁸.

Defende-se que a tutela coletiva preventiva (difusa) possa ser um meio para mudanças estruturais nessa dinâmica do ciberespaço, satisfazendo princípios como do acesso à justiça, por um grupo constitucionalmente protegido (os consumidores), bem como satisfaz a

⁴⁹⁴ *Ibid*, p. 68.

⁴⁹⁵ Os direitos coletivos em sentido estrito, por sua vez, são caracterizados também pela indivisibilidade, mas diferem dos direitos difusos na medida em que os titulares compartilham entre si ou com a parte contrária uma relação jurídica base independente do fato gerador da ação coletiva. (ROQUE, André. A tutela Coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais - LGPD. *Revista Eletrônica de Direito Processual*. Rio de Janeiro. Ano 13. Volume 20. Número 2. Maio a Agosto de 2019. p. 1-19. 2019. p. 5. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/redp/article/view/42138>. Acesso em 09 Feb 2023)

⁴⁹⁶ DIDIER, Freddie JR; ZANETI, Hermes JR. *loc. cit.*, p. 70.

⁴⁹⁷ ROQUE, André. *op. cit.*, p. 10.

⁴⁹⁸ MARTINS, Guilherme M; LONGHI, João Victor R. *loc. cit.*, p. 106.

indisponibilidade da demanda coletiva e reparação integral do dano. Sobre a indisponibilidade da demanda coletiva, os autores mencionam que “diferentemente do processo individual, no qual está presente a *facultas agendi* característica do direito subjetivo individual, o processo coletivo vem contaminado pela ideia de indisponibilidade do interesse público⁴⁹⁹”.

Dessa maneira, é dever dos legitimados ingressar com as tutelas coletivas para dirimir problemas estruturais dos serviços na *internet*. Os legitimados do artigo 82º do CDC podem propor, em nome próprio e no interesse das vítimas, ações coletivas de responsabilidade civil pelos danos sofridos, podendo ter um caráter preventivo (direitos difusos) ou repressivo (direitos individuais homogêneos).

Entende-se, portanto, que para mudanças estruturais as tutelas coletivas se apresentam como uma importante via. Desse modo, o judiciário cumpre seu papel constitucional de garantir o acesso à justiça e defesa dos consumidores, princípios constitucionais do Estado de Direito. Além do mais, a utilização da tutela coletiva pelos consumidores, podendo ser pelas associações ou pelos legitimados extraordinários, estimula a ideia de cidadania instrumental, ou seja, satisfaz o modelo de democracia deliberativa. Sendo assim, o judiciário passa a ser uma instância mais democrática e de diálogo. Este ideal é promovido pela Política Nacional das Relações de Consumo- PNRC⁵⁰⁰, presente nos artigos 4º e 5º do CDC.

Dessa maneira, a PNRC além de possuir uma função programática, atuará ativamente, satisfazendo seu objetivo de integrar uma rede de permanente diálogos políticos entre o Estado, a sociedade civil e os fornecedores. Assim, concretiza-se o ideal de solidariedade emancipatória para promover o princípio da harmonia das relações de consumo. Logo, verifica-se a PNRC como um compromisso tripartido entre os atores das relações de consumo, compartilhando a autoridade do Estado e, principalmente, resgatando a autoestima cívica de um grupo (no caso os consumidores) para a defesa dos seus interesses⁵⁰¹.

Portanto, em que pese as vias individuais de resolução de conflitos, essa satisfaz apenas um direito individual, não conseguindo dirimir problemas estruturais. Visando a satisfação de

⁴⁹⁹ *Ibid*, p. 109.

⁵⁰⁰ Essa política foi concebida com a finalidade de disciplinar o comportamento do Estado como grande mediador de interesses contrapostos da sociedade de consumo e dos agentes do mercado, concretizando o princípio da harmonia das relações de consumo de relevo constitucional pela compatibilização da livre iniciativa e da proteção do consumidor como pilares da ordem econômica, nos termos do artigo 170º, caput e seu inciso V, da Constituição Federal (VERBICARO, Dennis. A política nacional da relações de consumo como modelo de democracia deliberativa. *Revista Jurídica da Presidência Brasília* v. 19 n. 119 Out. 2017/Jan. 2018 p. 534-559. Dennis Verbicaro 535 <http://dx.doi.org/10.20499/2236-3645.RJP2018v19e119-1374>. Disponível em: <https://revistajuridica.presidencia.gov.br/index.php/saj/article/view/1374>. Acesso em 14 de Jan de 2022. p. 540)

⁵⁰¹ *Ibid*, p. 540.

uma harmonia nas relações de consumo é dever do Estado enfrentar as problemáticas de um determinado setor, como os oriundos da coleta desenfreada de dados pessoais em solo nacional. Para tanto, compreende-se que a tutela coletiva deve ser o instrumento utilizado para enfrentar essas questões.

SEÇÃO IV

3.3 POSSIBILIDADES DE TUTELA POSITIVA DA CONFIANÇA NO CIBERESPAÇO E A NECESSIDADE DE UMA ATUAÇÃO QUALIFICADA DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS.

Não há dúvidas que o consumidor enfrenta diversas vulnerabilidades ao navegar na *internet* provocando a necessidade de aprimorar a tutela positiva da confiança. Neste sentido, para demonstrar como a tutela positiva da confiança poderia dirimir vulnerabilidades no ciberespaço, explicar-se-á brevemente duas vulnerabilidades patentes nas relações digitais: a vulnerabilidade técnica-informacional e algorítmica.

O consumidor é um vulnerável técnico porque não possui os conhecimentos técnicos suficientes sobre os produtos e serviços que consome, confiando nas informações e funcionalidades apresentadas pelo fornecedor⁵⁰². Tal vulnerabilidade é clara na utilização dos serviços, pois muitas vezes o consumidor não entende e utiliza os serviços na sua completude. Sem se olvidar que os consumidores-médios não possuem conhecimento técnico sobre ciência da computação, programação e outros aspectos importantes dos serviços no ciberespaço.

Acentua essa ignorância a marcante vulnerabilidade informacional do usuário, pois como reflete Claudia Lima Marques “a distância física entre o fornecedor e o consumidor é enorme fator de debilidade informativa, as informações disponíveis são aquelas escolhidas pelo fornecedor e acessada com uniformidade⁵⁰³”.

⁵⁰² En atención a ello, se há construído a nivel doctrinario el concepto de vulnerabilidad técnica, en el entendido de que el usuario no posee los conocimientos suficientes respecto de los productos o servicios que contrata por oposición al proveedor, respecto de quien se presume los posee (SZAFIR, Dora; MARKS, Hillary. *loc. cit.*, p. 56)

⁵⁰³ MARQUES, Claudia Lima. *Confiança. loc. cit.*, p. 95.

É necessário lembrar que a informação é um direito básico do consumidor⁵⁰⁴, assim, o fornecedor possui um dever de conduta ativa de informar, sendo transparente em relação as condições do contrato e seus riscos⁵⁰⁵. Claudia Lima Marques elucida que informar é uma divisão de riscos entre as partes, ainda mais no meio digital⁵⁰⁶. Neste sentido, os deveres de informação dos fornecedores na *internet* são deveres de informar normais, especializados pelo meio, como o dever de transparência, de *disclosure* do produto ou serviço⁵⁰⁷. Sendo assim o consumidor é um vulnerável técnico-informacional do ciberespaço.

A vulnerabilidade técnica-informacional é um dos fatores da denominada vulnerabilidade algorítmica. A vulnerabilidade algorítmica pode ser entendida a partir da opacidade e injustiças da inteligência artificial (*vide capítulo 1*); suas violações aos direitos fundamentais do contraditório e devido processo legal.

A falta de *accountability* dos programadores e das plataformas colocam os consumidores em caixas-pretas, como já desenvolvido. O contexto torna-se mais pernicioso ao atestar a opacidade dos algoritmos, fazendo com que não se saiba as premissas do resultado (*opt out*)⁵⁰⁸. Muitas vezes, nem o próprio programador sabe explicar o porquê de determinado resultado e aliado a falsa percepção de neutralidade da máquina, o assunto torna-se muito mais complexo.

A opacidade interfere diretamente em direitos constitucionais, como o contraditório e o devido processo legal. A Constituição Federal dispõe sobre o contraditório (artigo 5º, inciso LV) e o devido processo legal (art. 5º, LIV) como direitos fundamentais dos cidadãos. Observa-se que, esses direitos estão um local diferenciado na carta magna por serem cláusulas pétreas, constando em um dos artigos mais importantes do texto constitucional.

Sem a possibilidade de entender como a máquina chegou a um resultado, o trabalhador e o consumidor não conseguem exercer de forma plena o seu contraditório, dificultando a impugnação do processo. Isto torna-se mais gravoso ao notar que a utilização de IA estão em

⁵⁰⁴O direito de informação do consumidor decorre da sua vulnerabilidade, uma vez que retrata a situação de submissão, de sujeição àquilo que é ofertado no mercado, ou seja, a sua situação de dependência em relação ao fornecedor e fragilidade na relação de consumo. O Código de Defesa do Consumidor tem por premissa proporcionar equilíbrio nas relações entre consumidor e fornecedor, daí porque a necessidade de transparência nesta relação. O fornecedor tem o dever legal de informar a parte em desvantagem a respeito dos dados fáticos, técnicos e científicos, que deverão estar presentes na oferta (BAGGIO, Andreza. *loc. cit.*, p. 53)

⁵⁰⁵ MARQUES, Claudia Lima. *op. cit.*, p. 246-247.

⁵⁰⁶ MARQUES, Claudia Lima. *Contratos...* *loc. cit.*, p. 189.

⁵⁰⁷ *Ibid*, p. 235.

⁵⁰⁸ NUNES, Dierle; MARQUES, Ana Luiza. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. *Revista dos tribunais online*, 2018. p. 430.

campos sensíveis, como em triagem de processos no judiciário, utilização na justiça criminal, contratações de empregos e concessões de créditos⁵⁰⁹. Neste sentido, é importante notar que a vulnerabilidade algorítmica do consumidor foi agravada com o veto do termo “pessoa natural” na disposição do artigo 20º da LGPD⁵¹⁰.

Além de todas as vulnerabilidades citadas, os usuários ainda são manipulados através do *design* dos sites e pela proliferação de *dark patterns*. Instrumentos utilizados pelos *players*, que induzem o consumidor a erro.

Com efeito, compreende-se que a dimensão positiva da confiança pode ser utilizada para impor aos *players* a obrigação de prestar informações qualificadas no momento dos avisos de consentimento. Por informações qualificadas entende-se que sejam claras e objetivas, sem excessos, informando pelo menos, o motivo do tratamento dos dados, a possibilidade ou não de compartilhamento com terceiros e seu ciclo de vida. Essa dimensão auxiliaria o princípio da finalidade e da informação, tão carentes nas atuais relações contratuais no ciberespaço.

Portanto, defende-se que a dimensão positiva da confiança pode ser materializada a partir dos conceitos de *privacy by design* e de *nudges*.

3.3.1 O conceito de racionalidade limitada e de *nudges*.

A teoria econômica clássica considera uma criatura ficcional chamada de *homo economicus* como todos os indivíduos, desse modo a premissa central é que as pessoas escolhem por otimização e que tais escolhas são imparciais⁵¹¹, assim, os indivíduos tomariam decisões sempre racionais. Contudo, uma ala de economistas, através de uma abordagem transdisciplinar com a psicologia, começa a questionar esse entendimento. Para economistas

⁵⁰⁹ NUNES, Dierle. A supervisão humana das decisões de inteligência artificial reduz riscos? *CONJUR*, 25.06.2021. Disponível em: [www.conjur.com.br/2021-jun-25/nunes-supervisao-humana-decisoes-ia-reduz-riscos#:~:text=A%20aposta%20que%20vem%20permeando,humanos%20que%20ser%C3%A3o%20encarregados%20de]. Acesso em: 29.06.2021.

⁵¹⁰ Embora a LGPD tenha regulamentado a matéria dos dados pessoais, a regulamentação de inteligência artificial é insipiente, não havendo uma menção no diploma legal sobre IA, apenas sobre decisão automatizada. No art. 20 do anteprojeto da LGPD, constava a possibilidade de revisão de decisão automatizada por pessoa natural (...) Todavia pressão dos setores empresariais devido ao custo que acarretaria uma pessoa para essa revisão, o termo “pessoa natural” foi vetado (VERBICARO, Dennis; MARANHÃO, Ney; CALANDRINI, Jorge. O impacto do capitalismo de plataforma no agravamento da vulnerabilidade algorítmica do consumidor e do trabalhador. *Revista de Direito do Trabalho*. Vol. 223. P. 277-305. Maio- Jun. 2022. p. 289)

⁵¹¹ THALER, Richard. *MISBEHAVING: A construção da economia comportamental*. Ed. Rio de Janeiro: Intrínseca, 2019, p. 279.

comportamentais existem diversos Fatores Supostamente Irrelevantes que influenciam nos momentos de decisões⁵¹², como de aceitar um contrato.

Herbet Simon, autor fundamental na economia e na área de inteligência artificial, ainda na década de 70, demonstra a existência de heurísticas que desmitificam o ideal do indivíduo sempre otimizando seu bem-estar. Simon identificou que o *homo sapiens* possui uma racionalidade limitada, desse modo, é limitado em apurar e interpretar informações ao tomar decisões, o que fazia o autor não acreditar que o indivíduo consiga maximizar seus objetivos em suas escolhas como preza a premissa da economia⁵¹³.

Para Simon, a economia buscou compreender apenas os resultados das escolhas e não o processo⁵¹⁴, fazendo com que se desconsidere importantes heurísticas nas tomadas de decisões que impossibilitam os indivíduos de tomarem sempre as melhores decisões. As heurísticas são consideradas atalhos mentais, facilitando as tomadas de decisões, fazendo com que o cérebro gaste menos energias para exercer escolhas⁵¹⁵. A partir da redução do esforço cognitivo, as heurísticas geram tomadas de decisões que muitas vezes não levam em consideração a lógica ou a probabilidade, gerando um ciclo vicioso e, conseqüentemente, levando os indivíduos a decisões ruins⁵¹⁶. Sendo assim, diferentemente do entendimento da teoria econômica, o *homo sapiens* não realiza suas escolhas segundo “expectativas racionais”, optando pela melhor escolha diante das opções⁵¹⁷.

Portanto, a partir dessa compreensão, economistas e psicólogos comportamentais começaram a pesquisar sobre forma de estimular comportamentos que otimizem o bem-estar dos indivíduos, desse modo, cria-se o conceito de *nudges*. Os *nudges* ou empurrão são intervenções por parte do Estado que visam preservar a autonomia e a liberdade das pessoas,

⁵¹² *Ibid*, p. 17 ss.

⁵¹³ STEINGRABER, Ronivaldo; FERNANDEZ, Ramon. A racionalidade limitada de Hebert Simon na Microeconomia. *Revista da Sociedade Brasileira de Economia Política*, São Paulo, nº 34, 2013. p. 137. Disponível em: <https://www.revistasep.org.br/index.php/SEP/article/view/5/80>. Acesso em 20 dez. 2021.

⁵¹⁴ Economics has largely been preoccupied with the *results* of rational choice rather than the *process* of choice. Yet as economic analysis acquires a broader concern with the dynamics of choice under uncertainty, it will become more and more essential to consider choice processes. In the past twenty years, there have been important advances in our understanding of procedural rationality. Particularly as a result of research in artificial intelligence and cognitive psychology. The importation of these theories of the processes of choice into economics could provide immense help in deepening our understanding of the dynamics of rationality, and of the influences upon choice of the institutional structure within which it takes place (SIMON, Hebert. Rationality as process of and as product of thought. *American Economic Review*, volume 68, number 2, 1978, p. 2-3, destaques do original. Disponível em: [https://josephmahoney.web.illinois.edu/BA504_Fall%202008/Session%208/Simon%20\(1978\).pdf](https://josephmahoney.web.illinois.edu/BA504_Fall%202008/Session%208/Simon%20(1978).pdf). Acesso em 20 dez. 2021.)

⁵¹⁵ VERBICARO, Dennis; CAÇAPIETRA, Ricardo. A economia comportamental no desenho de políticas públicas de consumo através das Nudges. *Revista de Direito do Consumidor*. vol. 133. ano 30. p. 385-411. São Paulo: Ed. RT, jan./fev. 2021, p. 397.

⁵¹⁶ *Ibid*. p. 398.

⁵¹⁷ THALER, Richard. *loc. cit.*, p. 19.

com o objetivo de auxiliar nas tomadas de decisões⁵¹⁸. Sendo assim, os empurrões atuam como mecanismos que direcionam as pessoas para determinados caminhos, mas, ao mesmo tempo, permite-se que os sujeitos possuam liberdade para exercer seu poder de escolha⁵¹⁹. Sendo assim, esse conceito atua como mecanismo sugestivo, assim, busca-se produzir um esclarecimento orientado, conduzindo os indivíduos a um estágio de bem-estar social.

Observa-se que a sua utilização na atualidade é considerável no ambiente social, seja para fins benéficos ou maléficis por agentes econômicos e, dessa forma, entende-se que o Estado pode utilizar as *nudges* para reprimir hábitos negativos dos agentes, assumindo um papel de arquiteto das escolhas para promover satisfação da população⁵²⁰. Sendo assim, a partir do entendimento da racionalidade limitada e das heurísticas que cercam os indivíduos nas tomadas de decisões, o Estado pode assumir o papel de arquiteto de escolhas para garantir o equilíbrio entre os agentes econômicos⁵²¹.

Os teóricos da *Behavioural Law and Economics* entendem que os agentes econômicos estão envoltos em uma série de armadilhas não declaradas, por isso, compete ao Estado, imbuído de sua missão social de buscar o bem-estar coletivo, ordenar as opções considerando os programas políticos previamente definidos no âmbito das políticas públicas. O agente econômico, além de estar submetido a um conjunto de informações limitadas, está, totalmente, influenciado por uma série de fatores que conduzem suas escolhas ao nível não ótimo. Para equilibrar o contexto das opções, a *Behavioural Law and Economics* sugere que o gestor das políticas públicas incorpore o papel de um “arquiteto das escolhas”⁵²².

Desta forma, as *nudges* são produzidas ou elaboradas para simplificar a vida das pessoas ou agregar maior segurança a elas⁵²³. De acordo com Sunstein, para que certa indução de comportamento seja considerada *nudge*, este incentivo deve preservar a liberdade de escolha do indivíduo, desse modo, impostos não são *nudges*, nem multas ou penas privativas de

⁵¹⁸ THALER, Richard H.; SUNSTEIN, Cass R. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New York: Penguin Publishing Group. Edição do Kindle, 2009.

⁵¹⁹ SOUZA, Luciana; RAMOS, Karen; PERDIGÃO, Sônia. Análise crítica da orientação de cidadãos como método para otimizar decisões públicas por meio da técnica nudges. *Rev. Bras. Polít. Públicas*, Brasília, v.8, n°2. 2018 p. 238. Disponível em: <https://publicacoes.uniceub.br/RBPP/article/view/5314>. Acesso em 09 Fev 2023.

⁵²⁰ RIBEIRO, Marcia Carla Pereira; DOMINGUES, Victor Hugo. Economia comportamental e direito: a racionalidade em mudança. *Rev. Bras. Polít. Públicas*, Brasília, v. 8, n° 2, 2018, p. 466. Disponível em: https://www.researchgate.net/publication/327893647_ECONOMIA_COMPORAMENTAL_E_DIREITO_A_RACIONALIDADE_EM_MUDANCA. Acesso em 09 Fev 2023.

⁵²¹ *Ibid*, p. 466. Grifo do original.

⁵²² *Ibid*, p. 466.

⁵²³ SOUZA, Luciana; RAMOS, Karen; PERDIGÃO, Sônia. *op. cit.*, p. 239.

liberdade⁵²⁴. O autor sustenta que às vezes a melhor escolha é aquela ativa, em outras palavras, uma abordagem onde se exige que as pessoas escolham, assim, garante-se que a vontade do agente seja exteriorizada e não haja imposições⁵²⁵.

Para Susteain, as *nudges* podem assumir diversas facetas, não havendo um padrão para todas. Desse modo, para o autor “Alguns empurrões funcionam porque informam as pessoas; outros empurrões funcionam porque facilitam certas escolhas, outros empurrões funcionam por causa do poder da inércia e da procrastinação⁵²⁶”.

Todavia, existem preocupações éticas na implementação desses incentivos comportamentais, razão pela qual as *nudges* possuem requisitos para sua utilização, tais como: promover o bem-estar, a autonomia e a dignidade. Desse modo, essas políticas não devem impor escolhas aos indivíduos e sim guiá-los, pois assim as *nudges* estariam descaracterizadas⁵²⁷.

Além disso, a utilização dos empurrões deve ser transparente, precedida de *accountability* e visando motivos lícitos⁵²⁸. Neste sentido, Thaler afirma que *nudges* não são *sludge*, em outras palavras, não servem para dificultar a vida dos indivíduos, como por exemplo, quando uma empresa oferece desconto aos consumidores que comprem um produto, mas exigem alta carga burocrática para o benefício, como enviar um formulário, uma cópia do recibo, o código de barra e outros requisitos que tornam essa ação demasiadamente complicada ou quando coloca-se um tempo para decidir sobre a compra de determinado produto⁵²⁹. Com efeito, Susteain e Thaler reconhecem que as *nudges* podem ser implementadas para motivos ilícitos, o que no ciberespaço pode ser percebido nas *dark patterns*⁵³⁰.

O que se nota no ciberespaço é que as plataformas utilizam vários *insights* de economia comportamental para influenciar os usuários de forma maléfica, especialmente, para coletar e tratar dados pessoais.

Verifica-se que as plataformas utilizam-se de *sludges* através do *design* para dificultar as escolhas dos usuários e, conseqüentemente, agravam o controle do fluxo de informação dos consumidores. O *sludge* mais conhecidos são as denominadas *Dark Patterns*.

⁵²⁴ SUSTEIN, Cass R. The Ethics of Nudging. *Yale Journal on Regulation*. Vol. 32, 2015, p. 417. Disponível em: [The Ethics of Nudging \(yale.edu\)](http://The Ethics of Nudging (yale.edu)). Acesso em 25 nov. 2021.

⁵²⁵ *Ibid*, p. 438.

⁵²⁶ *Some nudges work because they inform people; other nudges work because they make certain choices easier, still other nudges work because of the power of inertia and procrastination (Ibid, p. 417)*

⁵²⁷ SOUZA, Luciana; RAMOS, Karen; PERDIGÃO, Sônia. *op. cit.*, p. 238.

⁵²⁸ SUSTEIN, Cass. *op. cit.*, p. 428.

⁵²⁹ THALER, Richard H. *Nudge, not sludge*. *Science*, 2018. Disponível em: <https://science.sciencemag.org/content/361/6401/431.full>. Acesso em 20 dez. 2021.

⁵³⁰ IVANOVA, Irina. *How websites use “dark patterns” to manipulate you*. CBS News. 14 de maio de 2021. Disponível em: How websites use “dark patterns” to manipulate you - CBS News. Acesso em 20 dez 2021.

3.3.2 *Dark Patterns* ou padrões obscuros

As *Dark Patterns* ou padrões obscuros são metodologias danosas utilizadas contra os usuários pelas plataformas, que se utilizam da confiança e vulnerabilidade técnica-informacional do usuário para coletar dados pessoais.

As plataformas utilizam-se do *design* do seu *site*, *design* das notificações e outros artifícios para lucrar com a obtenção de dados. Em 2010, Harry Brignull, cunhou pela primeira vez o termo “*Dark Patterns*” e referia-se “imagine você administrar um negócio e pudesse apertar um botão para que seus clientes gastassem 21% a mais. É fácil⁵³¹”.

Desde então os padrões obscuros estão se desenvolvendo, desde fazer consumidores a comprarem o que não gostariam a impedir um controle das informações pessoais na *internet*⁵³². As *Dark patterns* ou padrões obscuros são manipulações que ocorrem no ciberespaço, caracterizando-se como *sludge*, fazendo com que consumidores façam coisas que não expressam sua real preferência⁵³³. A comunidade acadêmica já conceituou alguns dessas práticas de má-fé, como por exemplo, *trick question*, *sneak into Basket*, *roach motel*, *price comparison prevention*, *misdirection*, *hidden costs*, *confirmshaming*, *disguised ads*, e *friend spam*⁵³⁴.

À título de exemplo, o padrão obscuro denominado de *confirmshaming* ocorre quando o consumidor deseja cancelar um serviço e o site o faz confirmar pela segunda vez, causando uma espécie de constrangimento ao usuário⁵³⁵. Outro padrão muito utilizado é a *trick question*, que atua dificultando o exercício da vontade do usuário, mesmo de consumidores inteligentes. O *roach motel* ocorre quando é fácil entrar em um serviço, mas difícil de sair, como ocorre na exclusão de uma conta do Facebook ou na Amazon⁵³⁶.

⁵³¹ IVANOVA, Irina. *How websites use “dark patterns” to manipulate you*. CBS News. 14 de Maio de 2021. Disponível em: [How websites use “dark patterns” to manipulate you - CBS News](#). Acesso em 20 de Jul 2021.

⁵³² VERBICADO, Dennis; CALANDRINI, Jorge. *Nudges na proteção de dados pessoais no ciberespaço: um empurrão para uma decisão racional do consumidor*. *Revista de Direito do Consumidor*. Vol. 142. Ano 31. p. 185-214. São Paulo: Ed. RT, jul./ago. 2022, p.200.

⁵³³ LAGURI, Jamie; STRAHILEVITZ, Jacob. *Shining a Light on Dark Patterns*. *Journal of Legal Analysis*. Vol 13. Ed 1, 2021, p. 67. Disponível em: [OP-JLAJ200006 43..109 \(ssrn.com\)](#). Acesso em 25 de Jul 2021. p. 44.

⁵³⁴ DARK PATTERNS ORGANIZATION. *Types of dark patterns*. Disponível em: [Dark Patterns - Types of Dark Pattern](#). Acesso em 20 de Jul 2021.

⁵³⁵ LAGURI, Jamie; STRAHILEVITZ, Jacob. *op.cit.*, p. 48-49.

⁵³⁶ *Ibid*, p. 49.

Portanto, os padrões obscuros são artifícios utilizados pelos *players* que dificultam o exercício de uma autodeterminação informativa. Essas práticas influenciam o consumidor incidir em erro nos negócios jurídicos firmados na *internet*, violando a boa-fé e confiança contratual.

3.3.2.1 A eficácia dos padrões obscuros através de pesquisa científica randomizada

O artigo publicado na *Journal of Legal Analysis*, pelos autores Jamie Luguri e Lior Strahilevitz, questiona “O quanto as *dark patterns* são eficientes?”. Para os autores, os padrões obscuros estão tornando um pouco mais dolorosa as atividades na *internet*, sugando o tempo livre dos usuários quando estes não aceitam mais utilizar os serviços ou simplesmente queiram recusar determinadas solicitações das plataformas⁵³⁷.

O artigo publicado oferece importantes evidências sobre a eficiência dos padrões obscuros a partir de experimentos realizados com 1.963 adultos norte-americanos. O primeiro experimento utilizado pelos pesquisadores foi um teste A/B, onde apresenta-se diferentes tipos de possibilidades para grupos distintos, desse modo, é possível atestar como os usuários reagem a cada modelo. Neste sentido, havia um grupo de controle, cujo não foram expostos a padrões obscuros, e usuários que foram expostos a dois tipos de *dark patterns*: uma agressiva e outra moderada⁵³⁸.

Primeiro realizou-se perguntas referentes a dados pessoais, como gênero, idade, emprego e outros⁵³⁹. Após esses questionamentos, realizaram perguntas sobre o nível de preocupação pessoal com a privacidade na *internet*. Com a utilização de um *software* foi possível calcular quais participantes possuíam um alto “*score* de privacidade”⁵⁴⁰. Depois da coleta e tratamento desses dados foi oferecido um programa de proteção de dados pessoais e *score* de crédito⁵⁴¹.

⁵³⁷ IVANOVA, Irina. *How websites use “dark patterns” to manipulate you*. CBS News. 14 de Maio de 2021. Disponível em: [How websites use “dark patterns” to manipulate you - CBS News](#). Acesso em 20 de Jul 2021.

⁵³⁸ LAGURI, Jamie; STRAHILEVITZ, Jacob. *loc. cit.*, p. 59-60.

⁵³⁹ *Ibid*, p. 60.

⁵⁴⁰ *Ibid*, p. 61.

⁵⁴¹ Participants were then allowed to either accept or decline the data protection program. But the steps that were required to do so varied by the level of the dark pattern manipulation. In the control group condition, we did not include any dark patterns. As such, this condition serves as a baseline to help us establish a ceiling for what percentage of the sample was inherently interested in receiving the identity theft protection. Participants could thus either click “Accept” or “Decline” on the first screen. Regardless of which option they selected, they proceeded to the final stage of the experiment, which is described below (*Ibid*, p. 61)

É a partir da oferta do programa que se inicia a exposição dos usuários às *dark patterns*. Sendo assim, os usuários poderiam escolher duas opções “*Accept and continue (recommended)*” or “*Other options*”.

A Intenção era fazer que a aceitação ao programa fosse fácil, enquanto negar fosse mais complicado. Os autores ressaltam que ao utilizar a expressão “recomendando” utiliza-se um padrão obscuro, pois configura-se como uma heurística, onde os consumidores incidem no viés de recomendação ao confiarem na plataforma⁵⁴². Além disso, padrões obscuros como *confirmshaming*⁵⁴³, temporizador e *trick question*⁵⁴⁴ foram utilizados.

Na exposição a um agressivo padrão obscuro, as primeiras telas foram idênticas aos padrões obscuros moderados⁵⁴⁵, todavia, a diferença ocorria no processo de aceitação ou negação do programa de proteção de dados e crédito⁵⁴⁶. Os resultados dos estudos foram: 11.3% do grupo de controle, sem exposição a dark patterns, aceitaram o programa. Enquanto 25.8% do grupo exposto a moderada dark patterns aceitou o programa. Já os participantes expostos a um agressivo padrão obscuro tiveram aceitação de 41.9% ao programa de proteção de dados, resultando em um aumento de 371% em comparação com o grupo de controle⁵⁴⁷.

Percebe-se como a conclusão do experimento é preocupante, demonstrando como os usuários estão acostumados com as *dark patterns* no ambiente online, além de elucidar como

⁵⁴² LAGURI, Jamie; STRAHILEVITZ, Jacob. *op. cit.* p. 62.

⁵⁴³ If subjects selected “Other options,” they were directed to the next screen, which asked them to choose between “I do not want to protect my data or credit history” and “After reviewing my options, I would like to protect my privacy and receive data protection and credit history monitoring.” This question uses confirmshaming as a dark pattern to nudge respondents to accept the program (i.e. their decision to decline the program is framed as not wanting to protect their data) (*Ibid.*, p. 62)

⁵⁴⁴ If respondents chose to read more information (rather than accept the program), the next screen had information about why identity theft matters and what a thief could do with their personal information. The options and count down timer were the same as the previous screen. A third information screen explained how common identity theft is, with the same options and count down timer displayed before they could advance. The cumulative effect of these screens amounted to a nagging dark pattern. If participants endured all three information screens and chose “I would like to read more information,” they were then directed to a question designed to confuse them. They were asked, “If you decline this free service, our corporate partner won’t be able to help you protect your data. You will not receive identity theft protection, and you could become one of the millions of Americans who were victimized by identity theft last year. Are you sure you want to decline this free identity theft protection?” The two options were “No, cancel” and “Yes.” This trick question intentionally tried to confuse participants about which option they should select to decline the program. (*Ibid.*, p. 63)

⁵⁴⁵ *Ibid.*, p. 62.

⁵⁴⁶ Participants could either choose “Accept data protection plan and continue” or “I would like to read more information.” They were forced to remain on the page for at least ten seconds before being able to advance, and they were shown a countdown timer during this period. This screen created a significant roach motel. Namely, it obstructed respondents’ ability to decline the program by making it more onerous to decline than accept. It also toyed with respondents’ emotions by using vivid, frightening language in the text. For example, participants read that identity theft “can damage your credit status and cost you time and money to restore your good name.” (*Ibid.*, p. 62-63)

⁵⁴⁷ *Ibid.*, p. 64.

os padrões obscuros são extremamente eficientes em fazer com que consumidores realizem ações que não desejam. Os autores salientam a importância do artigo porque demonstra-se o poder desses padrões obscuros para a sociedade civil e acadêmica, mas ressaltam que “as empresas já sabem o resultado de pesquisas desse tipo através dos seus pesquisadores”⁵⁴⁸. Por fim, conclui-se que as manipulações através de padrões obscuros são extremamente competentes e seus efeitos são mais efetivos em adultos norte-americanos com menos educação, o que reforça desigualdades sociais na proteção de dados⁵⁴⁹.

Portanto, em função da racionalidade limitada, heurísticas, *sludges* e outros Fatores Supostamente Irrelevantes que impactam nas tomadas das decisões é importante partir para a criação de instrumentos coletivos de proteção de dados pessoais.

3.4 *Privacy by design* e os *nudges* como antídotos aos padrões obscuros

O “*Privacy by design*” fornece uma visão holística da privacidade⁵⁵⁰, pautando-se em princípios que devem ser aplicados para mitigar preocupações referentes à privacidade⁵⁵¹. O conceito não é novo, surgindo nos anos 70, e foi incorporado em 1990 na Diretiva Europeia de Proteção de Dados: a RL 95/46/EC⁵⁵².

A grande referência acadêmica dessa proposta é Ann Cavoukian., sendo reconhecida como a criadora do conceito de *Privacy by design (PbD)*⁵⁵³. Para Ann, a aplicação do conceito deve levar em considerações sete princípios, que são: A) proativo e não reativo, preventivo, não repressivo; B) privacidade como configuração padrão; C) privacidade incorporada ao design do site; D) funcionalidade completa, sem opacidades; E) Segurança de ponta a ponta; F) garantia de escolha e transparência e G) respeito pela privacidade do usuário através da confidencialidade⁵⁵⁴.

⁵⁴⁸ *Ibid*, p. 45.

⁵⁴⁹ LAGURI, Jamie; STRAHILEVITZ, Jacob. *op. cit.* p. 47.

⁵⁵⁰ MARRAFON, Marcos. *Privacy by Design* como princípio do direito à proteção de dados. *CONJUR*. 19 de Julho de 2021. Disponível em: ConJur - Privacy by design como princípio do direito à proteção de dados. Acesso em 23 dez. 2021.

⁵⁵¹ GURSES, Seda; CARMELA, Troncoso; DIAZ, Claudia. *Engineering Privacy by design*. K.U. Leuven/IBBT, ESAT/SCD-COSIC. Disponível em: Gurses-CPDP11.pdf (imdea.org). Acesso em 30 dez. 2021.

⁵⁵² MARRAFON, Marco; COUTINHO, Luiza. Princípio da Privacidade por Design: Fundamentos E Efetividade Regulatória Na Garantia Do Direito À Proteção De Dados. *Revista Eletrônica Direito e Política*, Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, Itajaí, v.15, n.3, 3º quadrimestre de 2020. Disponível em: www.univali.br/direitoepolitica - ISSN 1980-7791. p. 959.

⁵⁵³ MARRAFON, Marco; COUTINHO, Luiza. *Ibid*, p. 962.

⁵⁵⁴ *Ibid*, p. 964.

No cenário estadunidense, a *Federal Trade Commission* recomendou as companhias a adotarem o conceito do *privacy by design* para “promover a privacidade do consumidor em todas as suas organizações e em todas as fases do desenvolvimento dos seus produtos e serviços”⁵⁵⁵.

Fala-se de *Privacy by design* quando uma diretriz regulatória, como a LGPD, promove regras e princípios com o intuito de empregar uma tecnorregulação desde à concepção dos produtos e serviços. Por exemplo, *GDPR* traz em seu artigo 25º que a privacidade deve ser resguardada desde a fase de *design* até o fim da utilização pelo fornecedor⁵⁵⁶. Cots e Oliveira entendem que a LGPD atraiu o conceito de *Privacy by Design* no seu artigo 46º, parágrafo segundo ao estipular que “As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.”

Essa disposição impõe aos *players* a necessidade de pensar na privacidade dos seus clientes desde a concepção do serviço, preocupando-se com quais instrumentos utilizará para garantir a privacidade ainda na fase de criação. Nota-se a importância do princípio, que atua como um conceito preventivo, possuindo o condão de modificar atitudes negativas dos fornecedores ao estimular que os produtos e serviços garantam segurança antes de chegarem ao mercado e não após um *recall*.

O conceito, também, satisfaz a missão do CDC em garantir segurança aos serviços postos no mercado, como nota-se no caput do artigo 4º e seus incisos III e V, ambos dispositivos da Política Nacional de Relações de Consumo. Nesse mesmo sentido, é importante lembrar que o artigo 6º, I, do diploma garante a segurança dos serviços e produtos como um direito básico do consumidor. Por esta razão, o CDC oferece a possibilidade de o vulnerável responsabilizar os fornecedores em função do defeito do serviço e produto, conforme o art. 14º, § 1º e 12º, § 1º.

Além dessa faceta, compreende-se que o conceito pode satisfazer o princípio da informação, fundamental nas relações de consumo digital. Neste sentido, é possível impor aos *players* a necessidade de criar interfaces e *design* dos seus *sites* que beneficiem as boas decisões dos consumidores, apoiando os titulares em fazer boas escolhas. Outra possibilidade é utilizar o conceito para aprimorar os avisos de privacidade através do visual e o conteúdo do texto⁵⁵⁷.

⁵⁵⁵Promote consumer privacy throughout their organizations and at every stage of the development of their products and services (WONG, Richmond Y; MULLIGAN, Deirdre K. *Bringing Design to the Privacy Table*. Through the Lens of HCI. In CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, ACM, New York, NY, USA, 17 pages. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3290605.3300492>. Acesso em 08 de Fevereiro de 2022. p. 2.)

⁵⁵⁶MARRAFON, Marco; COUTINHO, Luiza. *op. Cit.*, p. 976.

⁵⁵⁷WONG, Richmond Y; MULLIGAN, Deirdre K. *op. cit.*, p 5.

Dessa maneira, o conceito atuaria como *nudges*, impulsionando os usuários a melhores decisões através da imposição de padrões e interfaces mais claras, objetivas e informativas nos *sites*. Como Sustain alude, alguns *nudges* podem ser essencialmente informativos ou que possuam padrões que facilitem empurrar os consumidores para melhores escolhas⁵⁵⁸. Neste sentido, o conceito de *privacy by design* e a aplicação das *nudges* visando uma arquitetura de escolha auxiliaria na promoção do controle de fluxo de informações pelos usuários.

A ideia de *nudges* aplicado para preocupações de privacidade não é nova, havendo diversos estudos que atestam a eficácia desse mecanismo contra barreiras comportamentais que fragilizam o poder de controle do fluxo informacional⁵⁵⁹. É neste sentido que as autoras entendem sobre a possibilidade de *nudges* para dirimir preocupações com privacidade, estabelecendo *standards* de práticas sobre coleta e tratamento na *internet*⁵⁶⁰.

Estudos internacionais apontam que o *design* das plataformas influencia diretamente no comportamento dos usuários, desse modo, *nudges* podem auxiliar o exercício de direitos de privacidade e personalidade dos usuários no ciberespaço⁵⁶¹. Tais abordagens são importantes pois garantem instrumentos coletivos de proteção de dados, visto que os instrumentos individuais se mostram fragilizados. Além disso, sabe-se que os indivíduos conferem diferentes valores sobre suas informações pessoais, dependendo muito do contexto⁵⁶², portanto é

⁵⁵⁸ SUSTEIN, Cass R. The Ethics of Nudging. *Yale Journal on Regulation*. Vol. 32, 2015, p. 417. Disponível em: The Ethics of Nudging (yale.edu). Acesso em 22 dez. 2021.

⁵⁵⁹ Tais obstáculos podem decorrer de uma combinação de fatores: preferências inconsistentes e quadros de julgamento; necessidades opostas ou contraditórias (como a necessidade de publicidade combinada com a necessidade de privacidade); informações incompletas sobre riscos, consequências ou soluções inerentes ao fornecimento (ou proteção) de informações pessoais; habilidades cognitivas limitadas que limitam nossa capacidade de considerar ou refletir sobre as consequências de ações relevantes para a privacidade; e vários desvios sistemáticos (e, portanto, previsíveis) do processo de decisão abstratamente racional. (ACQUISTI, Alessandro. Nudging Privacy: The Behavioral Economics of Personal Information. *Security & Privacy Economics*. November/December. 2009. p. 73. Tradução nossa)

⁵⁶⁰ ALMENDRA FREITAS, Cinthia O; ALMADA, Giovanna M. How can nudging solve some of the internet data privacy issues. *Direito e Desenvolvimento*, João Pessoa, v. 10, n. 2, p. 06-19, jul./dez. 2019. p. 14. Disponível em: <https://www.researchgate.net/publication/338093694> How can nudging solve some of the internet data privacy issues. Acesso em 09 Fev 2023.

⁵⁶¹ Neste sentido: ALMENDRA FREITAS, Cinthia O; ALMADA, Giovanna M. How can nudging solve some of the internet data privacy issues. *Direito e Desenvolvimento*, João Pessoa, v. 10, n. 2, p. 06-19, jul./dez. 2019. p. 14; Joint Research Centre, Institute for Prospective Technology Studies, Monteleone, S., Bavel, R., Esposito, G., et al., *Nudges to privacy behavior : explorando abordagens alternativas para avisos de privacidade*, Escritório de Publicações, 2015, <https://data.europa.eu/doi/10.2791/142795>.

⁵⁶² We've found that individuals assign radically different values to their personal information depending on whether they're focusing on protecting data from exposure or selling away data that would be otherwise protected (ACQUISTI, Alessandro. Nudging Privacy: The Behavioral Economics of Personal Information. *Security & Privacy Economics*. November/December. 2009. p. 73. Disponível em: <https://ieeexplore.ieee.org/document/5370707>. Acesso em: 09 Fev 2023)

necessário a criação de instrumentos coletivos para dirimir os riscos no *trade off* dos dados pessoais.

Diante dessa conjuntura de padrões obscuros, que dificultam o exercício da autonomia privada nas escolhas quanto a proteção de dados pessoais no ambiente online, incumbe ao Estado exercer seu papel de mediador nas relações de consumo digital, buscando satisfazer sua missão social de gerar bem-estar aos indivíduos e de proteger direitos fundamentais como a privacidade e personalidade. Por conseguinte, o Estado Regulador assumirá o papel de árbitro no mercado econômico para equilibrar a marcante assimetria que ocorre nas relações de consumo, ainda mais visíveis nas relações digitais em função da crescente exposição ao *marketing* comportamental e instrumentos rastreadores, que impedem o controle das informações pelo usuário, além da carência de informações e consentimento viciado que ocorre nesse ambiente⁵⁶³.

3.4.1 A implementação do princípio de *Privacy by design* e de *nudges* no Brasil

A tutela positiva da confiança relaciona-se com a preocupação em assegurar a expectativa do titular, impondo deveres de conduta, lealdade, boa-fé e confiança⁵⁶⁴. Sendo assim, a tutela positiva da confiança constitui uma força vinculante do contrato, impondo o cumprimento de deveres anexos e de conduta, além do respeito as legítimas expectativas dos contratantes.

Como reflete Marques um dos maiores *gap* das contratações na *internet* é alcançar a maior transparência nas condições gerais de contratação e de informações sobre os riscos, sendo um dos grandes desafios do comércio eletrônico⁵⁶⁵,

Neste sentido, entende-se que os conceitos defendidos podem satisfazer a tutela positiva da confiança ao impor deveres de conduta e a satisfação de deveres em anexo, como de informar. Sendo assim, o *privacy by design* e as *nudges* atuariam como forma de melhorar os avisos de privacidade, destacando as informações mais importantes, assim como impõe a necessidade de o *design* do *site* ser acessível.

Além disso, como apontam Cots e Oliveira, a LGPD atraiu o conceito de *Privacy by Design* no seu artigo 46º, sendo assim, os *players* que desejem colocar produtos e serviços no

⁵⁶³ VERBICARO, Dennis; CALANDRINI, Jorge. *loc. cit.*, p. 200.

⁵⁶⁴ MARQUES, Claudia Lima. *Contratos...* *loc. cit.*, p. 42.

⁵⁶⁵ Transparência e confiança andam juntas. Alcançar maior transparência nas condições gerais contratuais e nas informações sobre preços parece ser o grande desafio do comércio eletrônico hoje (MARQUES, Claudia Lima. *loc. cit.*, p. 141)

mercado de consumo brasileiro devem se preocupar desde a concepção com as questões de privacidade e proteção de dados. Como já desenvolvido em tópico anterior, essa disposição cumpre objetivos do CDC em relação à proteção da segurança dos consumidores.

Desse modo, existe algum instrumento no ordenamento jurídico que permite a implementação desses conceitos?

Defende-se que o CDC, em seus artigos 4º e 5º, traz a o instrumento propicio para ser vetor dessas Políticas Públicas, a Política Nacional das Relações de Consumo. A PNRC estabelece diretrizes e cria instrumentos que podem ser executados pelos órgãos integrantes do Sistema Nacional de Defesa do Consumidor - SNDC. Ressalta-se que a Secretaria Nacional do Consumidor - SENACON é o órgão que coordena o SNDC, sendo assim, a função da PNRC é a padronização da atuação do Estado, seus órgãos administrativos e da sociedade civil para dirimir a assimetria entre fornecedor e consumidor.

Portanto, o Estado poderá exercer esse papel através da instituição de *nudges* no ciberespaço, regulamentando arquiteturas de escolhas que permitam melhores tomadas de decisões dos usuários quanto a proteção dos seus dados pessoais, em especial, no fomento ao direito da autodeterminação informacional. Da mesma maneira, as plataformas devem optar por *design* de *sites* que favoreçam a proteção dos dados pessoais dos usuários, visto que a LGPD outorga a obrigação dos fornecedores de se adequarem ao melhor entendimento da lei⁵⁶⁶.

O objetivo dessa política nacional é a harmonização das relações de consumo⁵⁶⁷, com uma atuação em conjunto e qualificada com os atores do mercado (consumidor/fornecedor/Estado), buscando relações pautadas na boa-fé, confiança, transparência e informação⁵⁶⁸. O princípio da ação governamental é uma decorrência natural do reconhecimento da vulnerabilidade do consumidor, sendo assim, a instituição de Políticas Públicas são importantes instrumentos para a regulação Estatal em relações privadas assimétricas e violadoras de direitos, como as que ocorrem no ciberespaço. Desse modo, a partir do reconhecimento de uma problemática, como a da não satisfação do consentimento informado

⁵⁶⁶ O que se extrai do dispositivo legal acima mencionado é que, além da obrigação estatal quanto ao fomento de tais direitos, a legislação consumerista deve perseguir a preservação da qualidade, segurança, desempenho dos produtos e serviços que são colocados à disposição dos consumidores, a fim de que se atenda às suas necessidades descritas no artigo supramencionado, por meio de instrumentos de execução adequados e eficientes (OLIVINDO, Bruno S; SATANNA, Héctor V. Política Nacional de Relações de consumo: referencial para a concretização da proteção do consumidor. *Brazilian Journal of Development*. Curitiba, v.6, n.8, p.61543-61560.aug. 2020.ISSN 2525-8761. p. 61552. Disponível em: https://www.researchgate.net/publication/344559034_POLITICA_NACIONAL_DE_RELACOES_DE_CONSUMIDOR_REFERENCIAL_PARA_A_CONCRETIZACAO_DA_PROTECAO_DO_CONSUMIDOR. Acesso em 09 Fev 2023)

⁵⁶⁷ *Ibid*, p. 61552.

⁵⁶⁸ VERBICARO, Dennis; CALANDRINI, Jorge. *Nudges... loc. cit.*, p. 87.

como preconiza as leis, é possível uma Política Pública que vise dirimir essa questão através da PNRC⁵⁶⁹.

Essa disposição exprime dois importantes objetivos da PNRC: o fomento à um diálogo permanente entre os atores da relação e o compartilhamento da responsabilidade no mercado de consumo⁵⁷⁰. Neste sentido, entende-se a PNRC como uma autoridade compartilhada entre consumidores, fornecedores e Estado, visando o aperfeiçoamento e equilíbrio do mercado. Desse modo, o Estado deve assumir o papel de mediador de interesses contrapostos da sociedade de consumo e fornecedores, como é o caso do interesse de maior controle das informações por parte dos consumidores, enquanto as plataformas buscam maneiras de tratar mais dados para assediar o consumidor no ciberespaço⁵⁷¹.

Verifica-se, por conseguinte, a importância da PNRC para a criação de novas políticas públicas que busquem deixar o mercado menos agressivo, sendo um vetor importante para regulamentações no comércio eletrônico. Dessa maneira, o Estado pode atuar no seu papel regulador através do instrumento estabelecido no CDC, buscando criar e promover Políticas Públicas que tenham o condão de dirimir problemas enfrentados pelos consumidores, como no caso do tratamento dos seus dados pelos *players*. Como ensina Rodotá a proteção de dados pessoais deve ultrapassar a proteção individual para meios coletivos pois “a própria defesa da privacidade requer, portanto, um alargamento da perspectiva institucional, superando a lógica puramente proprietária e integrando os controles individuais com aqueles coletivos⁵⁷²”.

Neste sentido, entende-se que a PNRC pode ser o instrumento de implementação de coletivos de controle como as *nudges* e a aplicação do conceito de *privacy by design*. O art. 4º, II, alíneas “a” e “c”, dispõem sobre a atuação do Estado por a) iniciativa direta; ou b) pela sua presença no mercado de consumo, entre outras. Além disso, como explicado, a PNRC possui como princípio a harmonização das relações de consumo e a da ação governamental. Portanto, extrai-se das alíneas e dos princípios a possibilidade de intervenção reguladora do Estado, o

⁵⁶⁹ OLIVINDO, Bruno S; SATANNA, Héctor V. *op. cit.*, p. 61555.

⁵⁷⁰A Política Nacional das Relações de Consumo pode ser concebida, nessa perspectiva, como um compromisso tripartido entre o Estado, a sociedade civil e o empresário, promovendo não apenas um compartilhamento de poder do Estado, mas também buscando incentivar o resgate da autoestima cívica do grupo, que se vê como categoria de consumidores, possuindo melhores instrumentos para a defesa de seus interesses (VERBICARO, Dennis. A Política Nacional das Relações de Consumo como modelo de democracia deliberativa. *Revista Jurídica da Presidência Brasília* v. 19 n. 119 Out. 2017/Jan. 2018 p. 534-559. <http://dx.doi.org/10.20499/2236-3645.RJP2018v19e119-1374>. p. 540)

⁵⁷¹ VERBICARO, Dennis. A Construção de um novo modelo de cidadania participativa do consumidor a partir da Política Nacional das Relações de Consumo. *Revista de Direito do Consumidor* | vol 110/2017 | p. 311 - 339 | Mar – Abr/2017. p. 315

⁵⁷² RODOTÁ, Stefano. *loc. cit.*, p. 50.

que poderia ser realizado através da implementação das *nudges* e do conceito de *privacy by design* no ciberespaço a partir da PNR. Logo, há um arcabouço jurídico para a instituição desses controles coletivos⁵⁷³.

Dessa maneira, o Estado diante do seu papel de promover um crescimento socioeconômico não predatório, estaria autorizado a intervir no domínio econômico para “conduzir os comportamentos individuais a um nível socialmente desejado”⁵⁷⁴. Desse modo, os arquitetos de escolhas podem ajudar as pessoas a tomarem melhores decisões, afinal “O arquiteto de escolha tem a responsabilidade de organizar o contexto em que as pessoas tomam decisões”⁵⁷⁵.

Os *nudges* vêm ganhando espaço nas políticas públicas, principalmente, na Inglaterra e nos Estados Unidos, com programas que são um sucesso, como em questões de saúde⁵⁷⁶ e de previdência⁵⁷⁷. Por exemplo, *nudges* através de cores nas notificações de privacidade, destacando as informações importantes como: finalidade da coleta, quais os fins de tratamento, qual o ciclo de vida daqueles dados. Assim, as cores atuariam para chamar a atenção dos usuários. Observa-se que a Comissão Europeia ao realizar um experimento parecido concluiu que as mudanças na interface através do *design* mostram-se como uma importante via para dirimir riscos nos avisos de privacidade⁵⁷⁸.

Dessa maneira, além de um conceito de privacidade desde a concepção do *site*, as *nudges* através dos avisos de privacidade, que pode ser através das cores, por exemplo, apresentam-se como uma alternativa interessante para a promoção da autodeterminação informativa dos usuários, além de outras *nudges* no ciberespaço, que mostram-se importantes na satisfação do controle do fluxo de informações dos titulares.

Com a Política Nacional das Relações de Consumo e a LGPD, é possível a instituição das *nudges* no ciberespaço em solo nacional, e, desse modo, o Estado assume seu papel regulador no mercado de consumo, garantindo a defesa do consumidor.

4. A IMPORTÂNCIA DE UMA ATUAÇÃO QUALIFICADA DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS.

⁵⁷³ VERBICARO, Dennis; CALANDRINI, Jorge. *Nudges... loc. cit.*, p. 208.

⁵⁷⁴ VERBICARO; Dennis, CAÇAPIETRA, Ricardo. *loc cit.*, p. 399.

⁵⁷⁵ Choice architect has the responsibility for organizing the context in which people make decisions (*Ibid*, p. 399)

⁵⁷⁶ *Ibid*, p. 399.

⁵⁷⁷ THALER, Richard. *loc. cit.*, p. 321 e ss.

⁵⁷⁸ Joint Research Centre, Institute for Prospective Technology Studies, Monteleone, S., Bavel, R., Esposito, G., et al., *Nudges to privacy behavior : explorando abordagens alternativas para avisos de privacidade*, Escritório de Publicações, 2015, <https://data.europa.eu/doi/10.2791/142795>

4.1 As competências da ANPD.

Sabe-se que o processo de coleta e tratamento de dados é opaco e inacessível à comunidade em geral, o que resulta em uma caixa-preta. A relação no tratamento de dados é regida pela confiança graças à falta de *accountability* dos *players*, tornando um procedimento totalmente obscuro aos consumidores, restando apenas confiar que o tratamento daquela plataforma será conforme os princípios e as regras estabelecidas pelos diplomas legais⁵⁷⁹.

Diante dessa conjuntura, faz-se extremamente importante o protagonismo da ANPD na fiscalização das plataformas. A ANPD possui a força para impor que as plataformas adotem medidas de transparência para satisfazer as disposições das legislações de dados, além de ter a competência de editar regulamentos e procedimentos sobre a proteção de dados pessoais, incluindo a elaboração do relatório de impacto à proteção de dados conforme o estipulado no art. 55-J, XIII, da LGPD, bem como fiscalizar a realização dos testes de proporcionalidade realizados pelas empresas.

Neste sentido, o artigo 55-J, da LGPD, dispõe sobre a competência da ANPD de “elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade.” Além disso, a ANPD possui uma competência educativa, como nota-se na disposição do art. 55-J, VI, da LGPD “promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança”.

Sem falar, claro, da natureza fiscalizadora e sancionatória da ANPD prevista no inciso IV do artigo 55- J. Assim, a ANPD tem a competência de ouvir os agentes de tratamento para fins de prestação de contas (art. 55- J, XIV, LGPD), assim como, realizar auditorias (art. 55- J, XVI, da LGPD).

Todavia, o que se percebe é uma atuação tímida da ANPD, criando um ambiente de altos riscos para os usuários, visto que a fiscalização é incipiente, sem falar da ausência de uma Política Nacional de Dados Pessoais. Ressalte-se que apenas a ANPD possui a competência de sancionar as plataformas conforme o artigo 55-K da LGPD, sendo o órgão central e exclusivo na aplicação de sanções, prevalecendo sua decisão no que tange à violação de dados pessoais no Brasil⁷⁹.

⁵⁷⁹ VERBICARO, Dennis; CALANDRINI, Jorge. *A proteção. Loc. cit.*, p.93.

Em relação às sanções administrativas, que estão tipificadas no art. 52 da LGPD, a ANPD pode, por exemplo, multar em até 2% do faturamento da empresa em um limite de 50 milhões de reais por infração (art. 52, II, da LGPD). Pode, também, publicizar a infração para informar os usuários (art. 52, IV, da LGPD), bem como solicitar o bloqueio ou a eliminação dos dados pessoais que se referem à infração (art. 52, V e VI, da LGPD). Em casos mais graves, é possível a suspensão do tratamento total ou parcial e até a proibição, total ou parcial, do exercício de atividades relacionadas a tratamento de dados (art. 52, XI e XII, da LGPD).

Como desenvolvido, a Autoridade Nacional de Proteção de Dados é primordial para a efetividade dos princípios e garantias previstas na legislação e possui um papel relevante na elaboração de diretrizes que possam assegurar uma verdadeira conscientização da sociedade civil acerca do tratamento de dados pessoais⁵⁸⁰. Logo, verifica-se a importância de a Autoridade Nacional assumir o protagonismo no controle dos dados no ciberespaço, pois em razão da vulnerabilidade técnica do usuário, é praticamente impossível atestar violações sem a atuação da ANPD.

Nessa perspectiva, é fundamental resgatar a participação do Estado na confecção e execução (ao lado da sociedade civil e dos agentes econômicos) de uma verdadeira Política Nacional para a Tutela de Dados Pessoais no Brasil, implementando compromissos éticos, diretrizes para atuação das plataformas eletrônicas, tais como mecanismos de monitoramento periódico, modelos de *compliance* que valorizem não apenas a transparência na coleta e tratamento dos dados, mas também que imponham o dever ético de assumir, junto às autoridades e aos consumidores prejudicados, falhas de segurança e, desde logo, busquem assumir responsabilidades e mitigar os danos imediatamente causados e aqueles que ainda se materializarão no futuro, sem prejuízo da aplicação rigorosa das sanções administrativas previstas na LGPD.

Portanto, para que os direitos, as liberdades e a confiança dos consumidores sejam protegidos, é indispensável o protagonismo da ANPD, garantindo o controle no ciberespaço. Dessa maneira, a ANPD deve atuar no âmbito de suas competências preventiva e repressivamente, mediante a elaboração de relatórios de impacto, aplicando sanções administrativas, de maneira a moldar o comportamento das plataformas eletrônicas no sentido de se criar um ambiente corporativo transparente no uso das informações sensíveis do

⁵⁸⁰ MARTINS, Guilherme Magalhães; MARTINS, Plínio Lacerda; TOSTES, Eduardo Chow de Martino. Proteção dos dados pessoais no Brasil: a necessidade de especialização dos órgãos independentes de defesa do consumidor para uma atuação eficiente. Revista de Direito do Consumidor. vol. 134. ano 30. p. 137-173. São Paulo: Ed. RT, mar./abr. 2021. p. 144.

consumidor, a partir do reconhecimento de sua vulnerabilidade algorítmica; caso contrário, os benefícios sociais da legislação ficarão comprometidos.

4.2 Por uma Política Nacional de Proteção de Dados Pessoais no Brasil

Segundo o dicionário, a palavra cultura pode significar lavoura, vegetal cultivado, ato, arte, modo de cultivar, instrução, saber, estudo, apuro, perfeição, cuidado. Mormente, a palavra é utilizada para expressar um conjunto de normas de comportamento, saberes, hábitos, crenças, conjunto de saberes adquiridos⁵⁸¹.

Sendo assim, o sentido da palavra no presente trabalho é para expressar um modo de cultivar, de instrução, de preservar um conjunto de saberes adquiridos, visando um aperfeiçoamento da tutela de dados pessoais no Brasil.

É neste sentido que, Laura Mendes e Danilo Doneda, em artigo científico, entendem que a mudança cultural sobre a proteção de dados é um dos desafios atuais para a efetiva tutela desse Direito Fundamental⁵⁸². Assim, é imprescindível uma mudança cultural no entendimento da importância dos dados pessoais, compreendendo como os vazamentos podem gerar prejuízos patrimoniais e, principalmente, extrapatrimoniais aos titulares⁵⁸³. Concluindo, Danilo e Laura, entendem que a “efetiva aplicação da LGPD dependerá também de uma mudança cultural que compreenda que todo dado pessoal é merecedor de proteção jurídica⁵⁸⁴”. Para tanto, é necessária uma aplicação sistêmica da legislação com outros diplomas normativos que dispõem sobre o tema, aplicando a teoria do diálogo das fontes entre as leis setoriais, como CDC e LGPD.

Dessa maneira, incutir na sociedade brasileira a importância dos dados pessoais em razão do seu caráter personalíssimo é fundamental para a construção de uma cultura de dados

⁵⁸¹ DICIO. *Dicionário online de português*. Disponível em: <https://www.dicio.com.br/cultura/>. Acesso em 24 de Janeiro de 2022.

⁵⁸² MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*. vol. 120. ano 27. p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018.

⁵⁸³ Outro importante desafio diz respeito à mudança cultural, necessária para a eficaz implementação da Lei. Afinal, a LGPD traz os princípios da necessidade e da finalidade, que indicam que os dados pessoais somente poderão ser tratados quando o tratamento for necessário para atender às necessidades do controlador de dados e se a sua utilização ocorrer no âmbito do contexto ou de forma compatível com as finalidades para as quais os dados foram coletados. Isto é, faz-se necessária uma verdadeira mudança cultural para incorporarmos a compreensão de que todo dado pessoal é merecedor de proteção jurídica, por ser um meio de representação da pessoa na sociedade (*Ibid*, p. 474)

⁵⁸⁴ *Ibid*, p. 475.

personais. Criando, dessa maneira, um *standard* robusto de proteção e salvaguardas para os usuários⁵⁸⁵. Com efeito, entende-se a LGPD com um instrumento para estimular uma cultura de dados no Brasil⁵⁸⁶, o que deve ocorrer através da adoção de *compliance* nas empresas, absorvendo o conceito de *Privacy by design* e medidas preventivas.

Além disso, o Estado deve, no âmbito da Política Nacional das Relações de Consumo, prevista nos artigos 4º e 5º do CDC, incentivar, por exemplo, a educação e informação sobre o mercado de dados (art. 4º, IV, CDC). Para tanto, é importante uma atuação conjunta entre os órgãos de defesa do consumidor com a Autoridade Nacional de Proteção de Dados Pessoais.

Além desse papel educativo, é imprescindível um diálogo entre ANPD, MP, PROCON e outros órgãos para estabelecer diretrizes para a instrumentalização da LGPD, atuando proativamente. Neste sentido, defende-se uma maior atuação do Ministério Público e Defensorias com a ANPD, buscando uma cooperação com o objetivo de “tentar minimamente impedir os grandes abusos que podem ser cometidos pelas empresas que operam neste mundo virtual em detrimento dos consumidores brasileiros⁵⁸⁷”. Para Roque o MP ostenta um papel relevante na matéria de proteção de dados pessoais na esfera coletiva, inclusive para a instauração de inquéritos civis e a celebração de compromissos de ajustamento de conduta. Enquanto o autor aponta que a Defensoria Pública possui legitimidade quando se tratar de interesse de hipossuficientes⁵⁸⁸.

Além disso, como salienta Roque, não se pode olvidar que a, a Administração Pública possui legitimidade universal em matéria de tutela coletiva, valendo destacar que, nos termos do art. 82, III do CDC, esta abrange inclusive órgãos sem personalidade jurídica – o que inclui, naturalmente, a Autoridade Nacional de Proteção de Dados (ANPD), órgão integrante da

⁵⁸⁵ ÁVILA NEGRI, Sergio; KOKMAZ, Regina. A normatividade dos dados sensíveis na Lei Geral de Proteção De Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*. e-ISSN: 2526-0049. Goiânia, v. 5, n.1, p. 63-65. Jan/Jun, 2019. p. 81. Disponível em: <https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf>. Acesso em 24 de Janeiro de 2022.

⁵⁸⁶ *Ibid*, p.81.

⁵⁸⁷ A integração e a coordenação dos órgãos públicos do Brasil na proteção dos dados pessoais, citando aqueles com independência funcional, Ministério Público e Defensoria Pública juntamente da Autoridade Nacional de Proteção de Dados Pessoais, deve caminhar de forma organizada e estratégica, de maneira permanente e em constante evolução, para tentar minimamente impedir os grandes abusos que podem ser cometidos pelas empresas que operam neste mundo virtual em detrimento dos consumidores brasileiros. Revela-se ainda mais importante quando é observado que abusos podem ser de natureza e efeitos variados, seja afetando situações jurídicas individuais, normalmente nas relações de consumo, seja prejudicando a sociedade como um todo, com a manipulação das condutas e dos resultados eleitorais e democráticos do país (MARTINS, Guilherme Magalhães; MARTINS, Plínio Lacerda; TOSTES, Eduardo. *loc. cit.*, p. 151)

⁵⁸⁸ ROQUE, André. *loc. cit.*, p. 11.

Presidência da República (art. 55-A da LGPD, inserido pela Medida Provisória n.º 869/2018)⁵⁸⁹.

Nessa esteira, é fundamental uma atuação qualificada da ANPD, pois suas competências são de extrema importância para desenvolvimento de uma cultura de dados e para a aplicação da legislação.

Em relação a promoção de uma cultura de dados pessoais no Brasil, compreende-se a partir da leitura do artigo 55-J, da LGPD, que a ANPD possui competência para estimular e impor uma Política com esse fim. O artigo 55-J, da LGPD, dispõe que a ANPD pode “elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade.” Infirmo esse entendimento a competência de “promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança” (art. 55-J, VI, da LGPD).

Também, a ANPD deve estimular diálogos com os órgãos de defesa do consumidor através da Política Nacional das Relações de Consumo para, por exemplo, organizar: oficinas, palestras, eventos e estimular uma especialização dos funcionários⁵⁹⁰. Assim como, é importantíssimo a participação da sociedade civil, seja por meio de associações ou do interesse individual, fomentando o debate para uma necessária cultura de dados no Brasil.

Sem deixar de falar, claro, da natureza fiscalizadora e sancionatória da ANPD prevista no inciso IV do artigo 55- J. Assim, a ANPD tem a competência de ouvir os agentes de tratamento para fins de prestação de contas (art. 55- J, XIV, LGPD), assim como, realizar auditorias (art. 55- J, XVI, da LGPD).

É necessária essa promoção sobre a importância dessas informações, pois pesquisadores demonstram que as problemáticas sobre proteção de dados estão assumindo contornos sociais, onde as populações carentes, com menos acesso à informação estão sob mais riscos. Notou-se que a proteção em matéria de privacidade é mais comum nos grupos historicamente abastados,

⁵⁸⁹ *Ibid*, p. 12.

⁵⁹⁰ Ainda, a LGPD prevê expressamente a competência dos órgãos de defesa do consumidor para atuar, mediante requerimento do titular dos dados, no caso de infração dos seus direitos pelo controlador (artigo 18, § 8º), bem como o dever de articulação entre a Autoridade Nacional de Proteção de Dados e outros órgãos titulares de competência afeta à proteção de dados, como é o caso dos órgãos de defesa do consumidor (artigo 55-K, parágrafo único). (MARTINS, Guilherme M; LONGHI, João Victor R. *loc. cit.*, p. 105)

desse modo, se a informação não for difundida, haverá o agravamento de desigualdades já conhecidas agora na matéria de proteção de dados pessoais⁵⁹¹.

Sendo assim, o Brasil deve caminhar para o desenvolvimento e fortalecimento de uma Política Nacional de Proteção de Dados Pessoais, fomentando debate e educação para o aperfeiçoamento das práticas pelas empresas e, também, de aplicação da LGPD.

CONSIDERAÇÕES FINAIS:

Ao tratar da revolução tecnológica, especialmente no que tange ao objeto deste trabalho – comércio digital e dados –, busca-se demonstrar como se deu essa revolução e as transformações por ela provocadas. É importante conhecer a plataformização, o novo modelo de negócio consolidado, para entender como a *internet* participativa (*web 2.0*) impulsionou a relação dos usuários com os fornecedores, resultando na descoberta do denominado superávit comportamental.

O superávit comportamental permitiu às plataformas abordagens personalizadas por meio da publicidade direcionada, o que representou uma grande evolução para o *marketing*. A ciência mercadológica, aproveitando-se do *Big Data*, tornou-se a principal fonte de renda dos capitalistas de vigilância. Desse modo, em busca do lucro, as plataformas promovem um verdadeiro assédio de consumo aos usuários no ciberespaço, fragilizando e influenciando seus comportamentos.

Todo esse monitoramento constante das empresas sob seus consumidores para obter o “superávit comportamental”, resultou no denominado capitalismo de vigilância. Nesse contexto, as máquinas tornam-se os meios de produção. Desse modo, a IA é utilizada todos os dias nos novos serviços tecnológicos, classificando consumidores e predizendo suas ações, inclusive, tendo em vista a modulação algorítmica dos comportamentos dos usuários.

A problemática em torno da IA reside no fato de que essas tecnologias são inescrutáveis pela sociedade, enquanto o consumidor encontra-se translúcido no ciberespaço. Verifica-se o poder dos algoritmos em influenciar os comportamentos na *internet*, realizando uma modulação comportamental para os próprios benefícios das plataformas. Agrava-se esse cenário a

⁵⁹¹NARAYANAN, Arvind; REISMAN Dillon. *The Princeton web Transparency and accountability Project*. Transparent data mining dor Big and Small Data. Springer. 2017. Disponível em: [webtap-chapter.pdf](#) (princeton.edu). Acesso em 24 Janeiro 2022.

constatação de injustiças programadas pelos códigos, que acabam por perpetuar atitudes negativas pregressas da sociedade.

Conclui-se que em razão de tamanhos riscos presentes nos serviços tecnológicos postos no mercado de consumo é imperativo que o direito se adeque aos novos anseios da sociedade tecnológica, como ocorre com o desenvolvimento e aprofundamento da disciplina da proteção de dados pessoais pelo mundo, sendo fundamental, estender novas interpretações para a aplicação da legislação.

A seção II possui dois propósitos: falar do desenvolvimento da proteção de dados e sobre a tutela da confiança nas relações contratuais, sendo uma parte dogmática. Sendo assim, adentra-se nos fundamentos que compõe a matéria de proteção de dados, desse modo, aborda-se sobre a construção do direito de privacidade e seus múltiplos conceitos. Com efeito, desenvolve-se as diferentes concepções de privacidade, desde o entendimento do direito de ser deixado sozinho até os atuais entendimentos sobre o direito de privacidade, que se traduz no direito de controlar o fluxo das informações pessoais. Assim como, aprofunda-se no conceito de direitos de personalidade, perpassando pelo contexto histórico do seu desenvolvimento e consolidação como um direito a ser tutelado na ordem jurídica. Ainda, explica-se o direito à autodeterminação informativa a partir do julgamento do Tribunal Constitucional Alemão, em 1983.

Em seguida, realiza-se uma análise dos fundamentos da LGPD e dos direitos dos titulares preceituados pela legislação. Também, explica-se como se deu a consolidação da matéria de proteção de dados pessoais como um direito fundamental no ordenamento jurídico brasileiro, através do recorte de alguns votos dos Ministros que foram importantes no julgamento da ADI nº 6.389; apontando que essa perpetuação era um anseio e debate antigo da doutrina especializada.

O capítulo sobre a proteção da confiança nas relações contratuais inicia-se com o desenvolvimento do fator sociológico da confiança, entendendo a importância desse valor social para uma sociedade complexa. A partir dessa análise transdisciplinar, aborda-se sobre o desenvolvimento da teoria da confiança pelo direito privado, perpassando pelos negócios jurídicos e tutela da aparência. Neste sentido, demonstra-se as dimensões da proteção da confiança e sua relação com os princípios da boa-fé e função social do contrato. Após essa análise doutrinária, aponta-se o CDC como um diploma que protege amplamente a confiança dos seus tutelados.

Na seção III, após o aporte doutrinário anterior, objetiva-se demonstrar uma proteção de dados à luz da teoria da confiança, apontando como as plataformas investem em confiança

dos seus usuários, assim como, aproveitam-se desse valor, especialmente, nos momentos de tratamento dos dados pessoais. Sendo assim, analisa-se a problemática do consentimento e do legítimo interesse diante dos arranjos de um capitalismo de vigilância. A partir da demonstração dessas problemáticas, analisa-se ser necessário elevar em outra dimensão o respeito as legítimas expectativas dos titulares, como uma forma de interpretação mais benéfica ao vulnerável.

Entende-se que em todos os contratos de tratamento de dados no ciberespaço existem legítimas expectativas dos consumidores, como expectativas de privacidade e de proteção de dados. Tal conceito relaciona-se diretamente com a teoria da confiança, primordial para análise de negócios jurídicos e contratos- como os de tratamento de dados no ciberespaço. Logo, verifica-se um diálogo direto da teoria da confiança com a LGPD, buscando proteger as legítimas expectativas dos usuários.

Neste sentido, defende-se a possibilidade de responsabilização civil das plataformas nos casos de **a)** vazamento de dados; **b)** desvio de finalidade do tratamento. O fundamento da responsabilização é a frustração das legítimas expectativas dos titulares em segurança, privacidade e proteção de dados. Também, conclui-se que a tutela coletiva é um importante instrumento para possíveis mudanças estruturais, sendo uma via importantíssima para enfrentar os problemas do mercado de dados, que na maioria dos casos são coletivos.

A seção IV versa sobre a possibilidade de uma tutela coletiva da confiança através da instituição de princípios práticos e uma atuação mais sólida da ANPD. Visando não ficar limitado a tutela repressiva, buscou-se investigar maneiras de tutela preventiva na proteção de dados. Inicialmente, apresenta-se as dificuldades enfrentadas pelos usuários, como sua racionalidade limitada e a proliferação de *dark patterns* nas plataformas. Mas, ao mesmo tempo, propõe-se conceitos como antígenos à essas questões, apontando o *privacy by design* e *nudges* como possíveis soluções e sua maneira de instituição no ordenamento nacional.

Contudo, constata-se que isso só seria possível através de uma ANPD sólida, independente e atuando de maneira qualificada. Nessa esteira, verifica-se que as competências da ANPD a torna um órgão indispensável para a tutela de dados no Brasil. Contudo, reflete-se ser fundamental um diálogo da ANPD com outros órgãos e instituições de defesa do consumidor, pois a tarefa é árdua e necessita de amplos esforços. Neste sentido, defende-se a necessidade de uma Política Nacional de Proteção de Dados Pessoais, promovendo ações educativas, preventivas e repressivas para assegurar um respeito aos dados pessoais do cidadão brasileiro.

Com essas seções objetivou-se responder o problema proposto por essa dissertação: A manipulação da confiança dos usuários pelas plataformas fragiliza a sua autodeterminação informacional nos contratos de tratamento de dados pessoais?

Conclui-se que os *players* investem em confiança para angariar novos consumidores nos seus serviços, utilizando-se de ações publicitárias, métodos de classificação e outros instrumentos para tal. Ao mesmo tempo observa-se que as plataformas abusam da *fides* do usuário através de técnicas cibernéticas e comportamentais, atuando sem boa fé no *trade off* dos dados pessoais. Enquanto isso, verifica-se que confiar para o consumidor digital é inevitável em razão de toda a arquitetura dos modelos de negócio da *internet*.

Portanto, a partir do entendimento que é inevitável confiar para os usuários, e que as plataformas investem em confiança, assim como abusam desse valor, conclui-se que o consumidor se encontra em um estado de *hiperconfiança* no ciberespaço que o deixa *hipervulnerável*.

A hipervulnerabilidade do consumidor é clara diante dos instrumentos rastreadores, modulação comportamental, carência de informações, contratos de adesão e outras assimetrias enfrentadas pelos usuários. A partir de toda essa máquina, compreende-se que os *players* manipulam a confiança dos usuários nas relações negociais do ciberespaço, especialmente, no que tange aos contratos de tratamento de dados pessoais, pois atuam à margem das legislações sobre o tema.

Com todo esse cenário de manipulação da confiança do usuário conclui-se não ser possível falar em autodeterminação informacional, sendo um direito diretamente afetado pelas práticas de má-fé das plataformas que abusam da confiança dos seus consumidores.

A partir da constatação de um problema, a pesquisa investiga soluções para tutelar a confiança dos usuários nessas relações tão assimétricas. Dessa forma, defende-se a possibilidade de utilizar a dimensão negativa da confiança, isto é, de responsabilização na via individual e coletiva, assim como conclui-se ser necessário uma atuação positiva da confiança, que atuará de maneira preventiva. Para tanto, a ANPD mostra-se fundamental para a aplicação da LGPD em solo nacional.

REFERÊNCIAS

AFONSO, Luiz Fernando. *Proteção do consumidor: propaganda enganosa e prática do storytelling*. São Paulo: Almedina, 2020.

ACQUISTI, Alessandro. Nudging Privacy: The Behavioral Economics of Personal Information. *Security & Privacy Economics*. November/December. 2009. Disponível em: <https://ieeexplore.ieee.org/document/5370707>. Acesso em: 09 de Fev 2023.

AGRELA, Lucas. Facebook é último colocado em ranking de confiança de usuários. *Exame*, 24 set. 2020. Disponível em: <https://exame.com/tecnologia/facebook-e-ultimo-colocado-em-ranking-de-confianca-de-usuarios/>. Acesso em: 23 out. 2022.

AIRBNB. No negócio da confiança. *News*, 6 nov. 2019. Disponível em: <https://news.airbnb.com/br/no-negocio-da-confianca/>. Acesso em: 23 out. 2022.

ANDRADE, Fábio Siebeneichler de. A tutela dos direitos da personalidade no direito brasileiro em perspectiva atual. *Revista de Derecho Privado*, [s.l.], n. 24, p. 81-111, Enero-Junio 2013. Disponível em: https://repositorio.pucrs.br/dspace/bitstream/10923/11474/2/A_Tutela_dos_Direitos_da_Personalidade_no_Direito_Brasileiro_em_Perspectiva_Atual.pdf. Acesso em: 22 jan. 2022.

ALMENDRA FREITAS, Cinthia O; ALMADA, Giovanna M. How can nudging solve some of the internet data privacy issues. *Direito e Desenvolvimento*, João Pessoa, v. 10, n. 2, p. 06-19, jul./dez. 2019. Disponível em: https://www.researchgate.net/publication/338093694_How_can_nudging_solve_some_of_the_internet_data_privacy_issues. Acesso em 09 fev 2023.

ÁVILA NEGRI, Sergio; KOKMAZ, Regina. A normatividade dos dados sensíveis na Lei Geral de Proteção De Dados: ampliação conceitual e proteção da pessoa humana. *Revista de Direito, Governança e Novas Tecnologias*. e-ISSN: 2526-0049. Goiânia, v. 5, n.1, p. 63-65. Jan/Jun, 2019. p. 81. Disponível em: <https://indexlaw.org/index.php/revistadgnt/article/view/5479/pdf>. Acesso em: 24 de jan de 2022.

BAGGIO, Andreza Cristina. *O direito do consumidor brasileiro e a teoria da confiança*. São Paulo: Revista dos Tribunais, 2012.

BECK, Ulrich. *Sociedade de risco: rumo a uma outra modernidade*. São Paulo: Editora 34, 2011.

BENDICH, Albert M. Privacy, Poverty and the Constitution. *California Law Review*, Berkeley, v. 54, n. 2, p. 407-442, 1966. Disponível em: <https://lawcat.berkeley.edu/record/1110014>. Acesso em: 11 abr. 2022.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020.

BIONI, Bruno; KITAYAMA, Marina; RIELLI, Mariana. *O legítimo interesse na LGPD: quadro geral e exemplos de aplicação*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2021. Disponível em: https://www.researchgate.net/publication/352747913_O_LEGITIMO_INTERESSE_NA_LGPD_QUADRO_GERAL_E_EXEMPLOS_DE_APLICACAO_Associacao_Data_Privacy_Brasil_de_Pesquisa. Acesso em 09 Fev 2023.

BUCHAIN, Luiz Carlos. Proteção de dados: legítimo interesse e consentimento. *Revista da Faculdade de Direito da UFRGS*, Porto Alegre, n. 45, p. 106, 2021. Disponível em: <https://seer.ufrgs.br/revfacdir/article/view/107259>. Acesso em 09 Fev 2023.

BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção dos dados do consumidor*. São Paulo: Almedina, 2019.

BORGES, Gustavo; FILÓ, Maurício da Cunha S. Consumo, publicidade e inteligência artificial: (necessários) limites à tecnologia persuasiva no constante assédio do consumidor. *Revista de Direito do Consumidor*, São Paulo, v. 30, n. 136, p. 201-232, jul./ago. 2021.

BRANDEIS, Louis D. What Publicity Can Do. *Harper's Weekly*, USA, December 20, 1913, p. 10. Disponível em: http://3197d6d14b5f19f2f440-5e13d29c4c016cf96cbbfd197c579b45.r81.cf1.rackcdn.com/collection/papers/1910/1913_12_20_What_Publicity_Ca.pdf. Acesso em: 29 mar. 2022.

BRASIL. Lei n.º 8.078, de 11 de setembro de 1990. Institui o Código do Consumidor. *Diário Oficial da União*: seção 1, Brasília, DF, Suplemento, p. 1, 12 set. 1990. PL 3683/1989. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078.htm. Acesso em: 14 jan. 2022.

BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *Diário Oficial da União*: seção 1, Brasília, DF, p. 1, 11 jan. 2002. PL 634/1975. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 15 mar. 2022.

BRASIL. Decreto n.º 7.962, de 15 de março de 2013. Regulamenta a Lei n.º 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. *Diário Oficial da União*: seção 1, Brasília, DF, edição extra, p. 1, 15 mar. 2013. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/2013/decreto-7962-15-marco-2013-775557-publicacaooriginal-139266-pe.html>. Acesso em: 14 jan. 2022.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). *Diário Oficial da União*: seção 1, Brasília, DF, edição 157, p. 59, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 jan. 2022.

BRASIL. Supremo Tribunal Federal (Plenário). *Ação Direta de Inconstitucionalidade 6.389 DF 0090573-97.2020.1.00.0000*. Relatora: Min. Rosa Weber. Julgamento: 17 nov. 2020. Disponível em: <https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protECAo.pdf>. Acesso em: 27 set. 2022.

BROWN, Wendy. *Nas ruínas do neoliberalismo: a ascensão da política antidemocrática no Ocidente*. Tradução de Mario A. Marino, Eduardo Altheman C. Santos. São Paulo: Editora Filosófica Politeia, 2019.

BUOLAMWINI, Joy. Artificial Intelligence Has a Problem with Gender and Racial Bias. Here's How to Solve It. *Time*, Feb 7, 2019. Disponível em: <https://time.com/5520558/artificial-intelligence-racial-gender-bias/>. Acesso em: 15 mar. 2022.

CANARIS, Claus-Wilhelm. *Direitos fundamentais e direito privado*. Tradução de Ingo Wolfgang Sarlet e Paulo Mota Pinto. Coimbra: Almedina, 2003.

CASTELLS, Manuel. *Sociedade em rede*. Tradução de Roneide Venancio Majer. 8. ed. São Paulo: Paz e Terra, 1998.

CENTROS de distribuição da Nike. *Nike Careers*, [202-]. <https://jobs.nike.com/pt/distributioncenters>. Acesso em: 8 mar. 2022.

CHRISTENSEN, Clayton; RAYNOR, Michael E.; MCDONALD, Rory. What is Disruptive Innovation? *Harvard Business Review Magazine*, Dec. 2015. Disponível em: <https://hbr.org/2015/12/what-is-disruptive-innovation>. Acesso em: 8 mar. 2022.

COMÉRCIO eletrônico. *Gov.br*, Ministério das Relações Exteriores, 7 jul. 2020. Brasil. Disponível em: <https://www.gov.br/mre/pt-br/assuntos/politica-externa-comercial-e-economica/comercio-internacional/comercio-eletronico#:~:text=A%20Organiza%C3%A7%C3%A3o%20Mundial%20do%20Com%C3%A9rcio%20%28OMC%29%20define%20com%C3%A9rcio,fisicamente%20e%20que%20envolvem%20consumidores%2C%20firmas%20e%20governos%E2%80%9D>. Acesso em: 15 mar. 2022.

CORDEIRO, António Menezes. *Da boa fé no direito civil*. Lisboa: Almedina, 2017.

CORVALÁN, Juan Gustavo. Inteligencia Artificial GPT-3, Pretoria y Oráculos Algorítmicos en el Derecho. *International Journal of Digital Law*, Belo Horizonte, ano 1, n. 1, p. 11-52, jan./abr. 2020. Disponível em: https://www.researchgate.net/publication/347063344_Inteligencia_Artificial_GPT-3_Pretoria_y_Oraculos_Algoritmicos_en_el_Derecho_GPT-3_Artificial_Intelligence_Pretoria_and_Algorithmic_Oracles_in_Law. Acesso em 09 Feb 2023.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais*. 3. ed. São Paulo: Revista dos Tribunais, 2019.

DARK PATTERNS ORGANIZATION. *Types of dark patterns*. Disponível em: [Dark Patterns - Types of Dark Pattern](#). Acesso em 20 de Jul 2021.

DICIO. *Dicionário online de português*. Disponível em: <https://www.dicio.com.br/cultura/>. Acesso em 24 de Jan de 2022.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2021. *E-book*.

ERMANTRAUT, Victoria. Locação de algoritmos de inteligência artificial da Microsoft no Brasil: reflexões, dataficação e colonialismo. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021. p. 171-188.

FACEBOOK perde anunciantes e diz sofrer com “déficit de confiança”. *Canaltech*, 29 jun. 2020. Disponível em: <https://canaltech.com.br/publicidade/facebook-perde-anunciantes-e-diz-sofrer-com-deficit-de-confianca-167214/>. Acesso em: 23 out. 2022.

FACHIN, Luiz Edson; SILVA, Roberta Zumblick Martins da. Direito do consumidor, novas tecnologias e inclusão digital. *Revista de Direito do Consumidor*, São Paulo, n. 139, ano 31, p. 19-29, jan./fev. 2022.

FETCHENHAUER, Detlef; DUNNING, David. Do people trust too much or too little? *Journal of Economic Psychology*, [s.l.], n. 30, p. 263-276, 2009. Disponível em: . <https://sites.lsa.umich.edu/sasi/wp-content/uploads/sites/275/2015/11/fetchdunn.jep09.pdf>. Acesso em: 15 mar. 2022.

FLORIDI, Luciano. Ser humano e inteligência artificial: os próximos desafios do onlife. Entrevista concedida a Gian Paolo Terravecchia. Tradução de Moisés Sbardelotto. *Instituto Humanitas Unisinos*, 28 out. 2020. Disponível em: www.ihu.unisinos.br/78-noticias/604136-ser-humano-e-inteligencia-artificial-os-proximos-desafios-do-onlife-entrevista-com-luciano-floridi. Acesso em: 11 mar. 2021.

FRADA, Manuel A. Carneiro da. *Teoria da confiança e responsabilidade civil*. Lisboa: Almedina, 2015. Reimpressão da edição de fevereiro de 2004.

FRANEK, Kamil. How Facebook Makes Money: Business Model Explained. *Kamil Franek*, April 2021. Disponível em: <https://www.kamilfrank.com/how-facebook-makes-money-business-model-explained/>. Acesso em: 19 mar. 2022.

GIDDENS, Anthony. *As consequências da modernidade*. Tradução de Raul Fiker. São Paulo: Unesp, 1991.

GILLESPIE, Tarleton. The Platform Metaphor, Revisited. *Digital Society Blog*, 24 Aug. 2017. Disponível em: <https://www.hiig.de/en/the-platform-metaphor-revisited/>. Acesso em: 15 mar. 2022).

GURSES, Seda; CARMELA, Troncoso; DIAZ, Claudia. *Engineering Privacy by design*. K.U. Leuven/IBBT, ESAT/SCD-COSIC. Disponível em: [Gurses-CPDP11.pdf](https://www.imdea.org/files/Gurses-CPDP11.pdf) (imdea.org). Acesso em 30 dez. 2021.

HELMOND, Anne. The Platformization of the Web: Making Web Data Platform Ready. *Social Media + Society*, Sept. 30, 2015. Disponível em: <https://journals.sagepub.com/doi/10.1177/2056305115603080>. Acesso em: 15 mar. 2022.

HOW does YouTube make money? *Youtube*, [20--]. Disponível em: <https://www.youtube.com/howyoutubeworks/our-commitments/sharing-revenue/>. Acesso em: 19 mar. 2022.

IBM Developer. What is the Difference Between Deep Learning and Machine Learning? *Youtube*, 30 abr. 2020. 1 video (1:32). Disponível em: <https://www.youtube.com/watch?v=terWb6ja-HM>. Acesso em: 26 mar. 2022.

ILO. *World Employment and Social Outlook: The role of digital labour platforms in transforming the world of work*. Geneva: ILO, 2021. Disponível em: https://www.ilo.org/wcmsp5/groups/public/@dgreports/@dcomm/@publ/documents/publication/wcms_771749.pdf. Acesso em: 28 jun. 2021.

INGIZZA, Carolina. Vendas online no Brasil crescem 47% no 1º semestre, maior alta em 20 anos. *EXAME*, 27 ago. 2020. Disponível em: <https://exame.com/pme/e-commerce-brasil-cresce-47-primeiro-semester-alta-20-anos/>. Acesso em: 8 mar. 2022.

IVANOVA, Irina. *How websites use “dark patterns” to manipulate you*. CBS News. 14 de maio de 2021. Disponível em: [How websites use "dark patterns" to manipulate you - CBS News](https://www.cbsnews.com/news/how-websites-use-dark-patterns-to-manipulate-you/). Acesso em 20 dez 2021.

Joint Research Centre, Institute for Prospective Technology Studies, Monteleone, S., Bavel, R., Esposito, G., et al., *Nudges to privacy behavior : explorando abordagens alternativas para avisos de privacidade*, Escritório de Publicações, 2015, <https://data.europa.eu/doi/10.2791/142795>.

KNOTH, Pedro. Após ‘febre’ da compra coletiva, Peixe Urbano tem crise e está fora do ar. *Uol Economia*, 20 maio 2021. Disponível em: <https://economia.uol.com.br/noticias/redacao/2021/05/20/como-o-peixe-urbano-foi-de-queridinho-a-alvo-de-reclamacoes-em-uma-decada.htm>. Acesso em: 2 abr. 2022.

KRAMER, Adam D. I.; GUILLORY, James E.; HANCOCK, Jeffrey T. Experimental evidence of massive-scale emotional contagion through social networks. *In: PNAS Proceedings of the National Academy of Sciences of the United States of America*, v. 111, n. 24, p. 8788-8790, 2014. Disponível em: <https://www.pnas.org/doi/pdf/10.1073/pnas.1320040111>. Acesso em: 27 mar. 2022.

LACE, Susanne (ed.). *The Glass Consumer: Life in a surveillance society*. Bristol: Policy Press, 2005.

LAGURI, Jamie; STRAHILEVITZ, Jacob. Shining a Light on Dark Patterns. *Journal of Legal Analysis*. Vol 13. Ed 1, 2021, p. 67. Disponível em: [OP-JLAJ200006 43..109 \(ssrn.com\)](https://ssrn.com/abstract=3844444). Acesso em 25 de Jul 2021.

LARENZ, Karl. *Metodologia da ciência do direito*. 3. ed. Lisboa: Fundação Calouste Gulbenkian, 1997.

LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999.

LIPOVETSKY, Gilles. *A felicidade paradoxal: ensaio sobre a sociedade de hiperconsumo*. São Paulo: Companhia das Letras, 2007.

LOPES, Marco Antônio. Alphabet, dona do Google (GOGL34): lucro sobre e receita supera consenso; ações disparam. *Suno notícias*, 1.º fev. 2022. Disponível em:

<https://www.suno.com.br/noticias/alphabet-google-lucro-sobe-receita-4t21/>. Acesso em: 31 mar. 2022.

LOPES, Maria Elisabete Vilaça. O consumidor e a publicidade. *Revista de Direito do Consumidor*, São Paulo, n. 1, p. 149-183, mar. 1992.

MACHADO, Débora Franco. A colonização dos dados como produto das operações das mídias sociais no Sul global. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021. p. 53-68.

MAGNANI, Vitor. Físico e Digital: O futuro do comércio é “online to offline”. *Forbes*, 21 out. 2021. Brasil. Disponível em: <https://forbes.com.br/forbes-tech/2021/10/fisico-e-digital-o-futuro-do-comercio-e-online-to-offline/#:~:text=Apenas%20%25%20de%20todo%20varejo,final%20do%20ano%20de%202021>. Acesso em: 8 mar. 2022.

MARÍÑEZ SÁNCHEZ, César David. La confianza: aproximaciones teóricas y propuesta sistémica para su abordaje en las ciencias sociales. *Século XXI: Revista de Ciências Sociais*, Santa Maria, RS, v. 2, n. 1, p. 168-199, jan./jun. 2012.

MARQUES, Claudia Lima. *Confiança no comércio eletrônico e a proteção do consumidor*. São Paulo: Revista dos Tribunais, 2004.

MARQUES, Claudia Lima. Proteção do consumidor no comércio eletrônico e a chamada nova crise do contrato: por um direito do consumidor aprofundado. *Revista de Direito do Consumidor*, São Paulo, v. 15, n. 57, p. 9-59, jan./mar. 2006.

MARQUES, Claudia Lima. *Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais*. 8. ed. São Paulo: Revista dos Tribunais, 2016.

MARQUES, Claudia Lima; MIRAGEM, Bruno. *O novo direito privado e a proteção dos vulneráveis*. São Paulo: Revista dos Tribunais, 2014.

MARRAFON, Marco; COUTINHO, Luiza. Princípio da Privacidade por Design: Fundamentos E Efetividade Regulatória Na Garantia Do Direito À Proteção De Dados. *Revista Eletrônica Direito e Política*, Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, Itajaí, v.15, n.3, 3º quadrimestre de 2020. Disponível em: www.univali.br/direitoepolitica - ISSN 1980-7791. Acesso em: 09 Fev 2023;

MARRAFON, Marcos. Privacy by Design como princípio do direito à proteção de dados. *CONJUR*. 19 de Julho de 2021. Disponível em: [ConJur - Privacy by design como princípio do direito à proteção de dados](https://www.conjur.com.br/2021-jul-19-privacy-by-design-como-principio-do-direito-a-protecao-de-dados). Acesso em: 23 dez. 2021.

MARTINS, Rafael. Apontamentos sobre a confiança legítima no Direito brasileiro. *Revista da EMERJ*, Rio de Janeiro, v. 10, n. 40, p. 177-190, 2007. Disponível em: <https://core.ac.uk/download/16041019.pdf>. Acesso em: 09 Fev 2023.

MARTINS, Guilherme M; LONGHI, João Victor R. Responsabilidade Civil na Lei Geral de Proteção de Dados, Consumo e a Intensificação Da Proteção Da Pessoa Humana Na Internet. *Revista de Direito do Consumidor*. Vol. 139. p. 101-124. Jan- Fev. 2022.

MARTINS, Guilherme M. Confiança e aparência nos contratos eletrônicos de consumo via internet. *Doutrinas Essenciais de Responsabilidade Civil*. São Paulo: Ed. RT. Vol. 8. p. 1311-1342. Out. 2011.

MARTINS, Guilherme Magalhães; MARTINS, Plínio Lacerda; TOSTES, Eduardo Chow de Martino. Proteção dos dados pessoais no Brasil: a necessidade de especialização dos órgãos independentes de defesa do consumidor para uma atuação eficiente. *Revista de Direito do Consumidor*. vol. 134. ano 30. p. 137-173. São Paulo: Ed. RT, mar./abr. 2021.

MARTINS-COSTA, Judith. Princípio da confiança legítima e princípio da boa-fé objetiva. Termo de Compromisso de Cessação (TCC) ajustado ao Cade. Critérios da interpretação contratual: os “sistemas de referência extracontratuais” (“circunstâncias do caso”) e sua função no quadro semântico da conduta devida. Princípio da unidade ou coerência hermenêutica e “usos do tráfego”. Adimplemento Contratual. *Revista dos Tribunais*, São Paulo, v. 95, n. 852, p. 87-126, out. 2006.

MATTIUZZO, Marcela; PONCE, Paula. O legítimo interesse e o teste da proporcionalidade: uma proposta interpretativa. *Internet & sociedade*, v. 1, n. 2, p. 57, dez. 2020. Disponível em: https://www.researchgate.net/publication/359510043_O_legitimo_interesse_e_o_teste_da_proporcionalidade_uma_proposta_interpretativa. Acesso em 09 de fev de 2023.

MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Universidade de Brasília, DF, 2008. Disponível em: <https://repositorio.unb.br/handle/10482/4782>. Acesso em: 11 abr. 2022.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. *Revista de Direito do Consumidor*. vol. 120. ano 27. p. 469-483. São Paulo: Ed. RT, nov.-dez. 2018

MENDES, Laura Schertel. A Lei Geral de Proteção de Dados Pessoais: um modelo de aplicação em três níveis. *Revista dos Tribunais*, São Paulo, v. 108, n. 1009, caderno especial LGPD, p. 35-56, nov. 2019. Disponível em: https://www.academia.edu/42741177/A_lei_geral_de_prote%C3%A7%C3%A3o_de_dados_pessoais_um_modelo_de_tr%C3%AAs_n%C3%ADveis . Acesso em: 17 set. 2022.

MILHOMENS, Heitor Antunes. *Tutela da confiança e da vulnerabilidade na economia do compartilhamento: empoderamento do consumidor digital e mitigação da vulnerabilidade estrutural na era do hiperconsumo*. 2021. 228 f. Dissertação (Mestrado em Direito) – Universidade Federal do Pará, Belém, 2021.

MIRAGEM, Bruno. Diretrizes interpretativas da função social do contrato. In: MIRAGEM, Bruno; MARQUES, Claudia Lima (org.). *Doutrinas essenciais: Direito do Consumidor*. São Paulo: Revista dos Tribunais, 2011. v. 1, p. 133-160.

MIRAGEM, Bruno. *Curso de direito do consumidor*. 4. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2013.

MIRAGEM, Bruno. Novo paradigma tecnológico, mercado de consumo digital e o direito do consumidor. *Revista de Direito do Consumidor*, São Paulo, v. 125, ano 28, p. 17-62, 2019.

Disponível em:

<https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1243/1168>. Acesso em: 9 abr. 2022.

MORAES, Maria Celina Bodin de. Danos à pessoa humana: uma leitura civil-constitucional dos danos morais. In: SARLET, Ingo Wolfgang (org.). *Constituição, direitos fundamentais e direito privado*. 2. ed. Porto Alegre: Livraria do Advogado, 2006. p. 59-140.

MORRIS, Ian. Facebook Knows When You Fall in Love, And That's Pretty Creepy. *Forbes*, Dec. 31, 2016. Disponível em: <https://www.forbes.com/sites/ianmorris/2016/12/31/facebook-knows-when-you-fall-in-love-and-thats-pretty-creepy/#51fef6c16f52>. Acesso em: 29 jun. 2021.

MUCELIN, Guilherme. *Conexão online e hiperconfiança: os players da economia do compartilhamento e o direito do consumidor*. São Paulo: Revista dos Tribunais, 2020. *E-book*.

MURPHY, Andrea; HAVERSTOCK, Elisa; GARA, Antoine; HELMAN, Chris; VARDI, Nathan. Global 2000: as maiores empresas de capital aberto do mundo em 2021. *Forbes*, 13 maio 2021. Disponível em: <https://forbes.com.br/forbes-money/2021/05/global-2000-as-maiores-empresas-de-capital-aberto-do-mundo-em-2021/>. Acesso em: 30 set. 2021.

NALIN, Paulo. A função social do contrato no futuro Código Civil brasileiro. *Revista de Direito Privado*, São Paulo, v. 3, n. 12, p. 50-60, out./dez. 2002.

NARAYANAN, Arvind; REISMAN, Dillon. The Princeton Web Transparency and Accountability Project. In: CERQUITELLI, Tania; QUERCIA, Daniele; PASQUALE, Frank (ed.). *Transparent data mining for Big and Small Data*. [S.l.]: Springer, 2017. p. 1-24. Disponível em: <https://www.cs.princeton.edu/~arvindn/publications/webtap-chapter.pdf>. Acesso em: 15 mar. 2022.

NISSENBAUM, Helen. Privacy as Contextual Integrity. *Washington Law Review*, [s.l.], v. 79, n. 1, p. 119-157, 2004.

NISSENBAUM, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. [S.l.]: Stanford Law Books, 2010.

NIEVA, Ricardo. Navegador no aplicativo do TikTok inclui código que pode monitorar suas teclas digitadas, diz pesquisador. *FORBES*. Estados Unidos. 18 de agosto de 2022.

Disponível em: <https://www.forbes.com/sites/richardnieva/2022/08/18/tiktok-in-app-browser-research/?sh=3e5ccabc7c55>. Acesso em 12 de jande 2023.

NORONHA, Fernando. *O direito dos contratos e seus princípios fundamentais: autonomia privada, boa-fé, justiça contratual*. São Paulo: Saraiva, 1994.

NOVA campanha da Uber dá protagonismo às pessoas. *Promoview*, 17 maio 2018.

Disponível em: <https://www.promoview.com.br/categoria/publicidade/nova-campanha-da-uber-da-protagonismo-as-pessoas.html>. Acesso em: 23 out. 2022.

NUNES, Dierle; MARQUES, Ana Luiza Pinto Coelho. Inteligência artificial e direito processual: vieses algorítmicos e os riscos de atribuição de função decisória às máquinas. *Revista de Processo*, São Paulo, v. 43, n. 285, p. 421-447, nov. 2018.

NUNES, Dierle. A supervisão humana das decisões de inteligência artificial reduz riscos? *CONJUR*, 25.06.2021. Disponível em: [www.conjur.com.br/2021-jun-25/nunes-supervisao-humana-decisoes-ia-reduz-riscos#:~:text=A%20aposta%20que%20vem%20permeando,humanos%20que%20ser%C3%A3o%20encarregados%20de]. Acesso em: 29.06.2021.

OLIVEIRA, Ricardo; COTS, Márcio. O legítimo interesse. In: OLIVEIRA, Ricardo; COTS, Márcio, coordenação. *O legítimo interesse e a LGPD*. 2. Ed. Ver., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021.

OLIVINDO, Bruno S; SATANNA, Héctor V. Política Nacional de Relações de consumo: referencial para a concretização da proteção do consumidor. *Brazilian Journal of Development*. Curitiba, v.6, n.8, p.61543-61560. aug. 2020. ISSN 2525-8761. Disponível em: https://www.researchgate.net/publication/344559034_POLITICA_NACIONAL_DE_RELACOES_DE_CONSUMO_REFERENCIAL_PARA_A_CONCRETIZACAO_DA_PROTECAO_DO_CONSUMIDOR. Acesso em 09 Fev 2023.

O'NEIL, Cathy. *Algoritmos de destruição em massa: como o Big Data aumenta a desigualdade e ameaça a democracia*. Tradução de Rafael Abraham. Santo André, SP: Editora Rua de Sabão, 2020.

PASQUALE, Frank. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press, 2015.

PASQUALE, Frank. *The Automated Public Sphere*. University of Maryland, Francis King Carey School of Law Legal Studies, Research Paper No. 2017-31. Nov. 10, 2017, p. 10. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3067552. Acesso em: 2 abr. 2022.

PESQUISA mostra que 82,7% dos domicílios brasileiros têm acesso à internet. *Ministério das Comunicações*, 14 abr. 2021. Disponível em: <https://www.gov.br/mcom/pt-br/noticias/2021/abril/pesquisa-mostra-que-82-7-dos-domicilios-brasileiros-tem-acesso-a-internet#:~:text=IBGE->, Pesquisa%20mostra%20que%2082%2C7%25%20dos%20domic%C3%ADlios,brasileiros%20t%C3%AAm%20acesso%20%C3%A0%20internet&text=A%20popula%C3%A7%C3%A3o%20brasileira%20est%C3%A1%20cada,Geografia%20e%20Estat%C3%ADstica%20(IBGE). Acesso em: 18 mar. 2022.

PIFFERO, Luiza. Confiança: por que é importante e porque pode te prejudicar. *GZH Comportamento*, 29 nov. 2019. Disponível em: <https://gauchazh.clicrbs.com.br/comportamento/noticia/2019/11/confianca-por-que-e-importante-e-por-que-pode-te-prejudicar-ck3k3o9mm00yy01rzgyvfmap6.html>. Acesso em: 15 out. 2022.

POELL, Thomas; NIEBORG, David; VAN DIJCK, José. Plataformização. *Revista Fronteiras: estudos midiáticos*, Porto Alegre, v. 22, n. 1, p. 2-10, jan./abr. 2020. Disponível em: https://www.researchgate.net/publication/341921979_Plataformizacao. Acesso em 09 Fev 2023.

PRADO, Filipe. Comércio social deve movimentar US\$ 1,2 trilhão em 2025, indica pesquisa. *Istoé Dinheiro*, 11 jna. 2022. São Paulo. Disponível em: <https://www.istoedinheiro.com.br/comercio-social-deve-movimentar-u-12-trilhao-em-2025-indica-pesquisa/>. Acesso em: 14 mar. 2022.

PROTEÇÃO de dados pessoais passa a ser direito fundamental. *CONJUR*, 10 fev. 2022. Disponível em: <https://www.conjur.com.br/2022-fev-10/protecao-dados-pessoais-passa-direito-constitucional>. Acesso em: 23 fev. 2022.

RECHAZAN información sobre el traslado de Nike de sus fábricas de Vietnam. *Vietnam Plus*, 5 out. 2021. Disponível em: <https://es.vietnamplus.vn/rechazan-informacion-sobre-el-traslado-de-nike-de-sus-fabricas-de-vietnam/142024.vnp>. Acesso em: 8 mar. 2022.

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

RODRIGUES, Léo Peixoto; NEVES, Fabrício Monteiro. *A sociologia de Niklas Luhmann*. Petrópolis, RJ: Vozes, 2017.

ROQUE, André. A tutela Coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD). *Revista Eletrônica de Direito Processual*. Rio de Janeiro. Ano 13. Volume 20. Número 2. maio a agosto de 2019. p. 1-19. 2019. Disponível em: <https://www.e-publicacoes.uerj.br/index.php/redp/article/view/42138>. Acesso em: 09 Fev 2023.

ROSA, Bruna. Apple lança primeira campanha sobre privacidade de dados no Brasil e em mais 23 países. *O Globo*, 26 maio 2022. Disponível em: <https://oglobo.globo.com/economia/tecnologia/noticia/2022/05/apple-lanca-primeira-campanha-sobre-privacidade-de-dados-no-brasil-e-em-mais-23-paises.ghtml>. Acesso em: 23 out. de 2022.

RIBEIRO, Marcia Carla Pereira; DOMINGUES, Victor Hugo. Economia comportamental e direito: a racionalidade em mudança. *Rev. Bras. Polít. Públicas*, Brasília, v. 8, nº 2, 2018. Disponível em: https://www.researchgate.net/publication/327893647_ECONOMIA_COMPORAMENTAL_E_DIREITO_A_RACIONALIDADE_EM_MUDANCA. Acesso em 09 Fev 2023.

SARMENTO, Daniel. *Livres e iguais: estudos de Direito Constitucional*. Rio de Janeiro: Lumen Juris, 2006.

SARMENTO, Daniel. *Direitos fundamentais e relações privadas*. 2. ed. Rio de Janeiro: Lumen Juris, 2010.

SCHMIDT NETO, André Perin. *Contratos na sociedade de consumo: vontade e confiança*. 2. ed. São Paulo: Revista dos Tribunais, 2019. *E-book*.

SILVA, Tarcízio. Colonialidade difusa no aprendizado de máquina: camadas de opacidade algorítmica na Imagenet. *In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, 2021. p. 87-107.*

SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. *In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, 2021. p. 33-51.*

SOUZA, Luciana; RAMOS, Karen, PERDIGÃO, Sônia. Análise crítica da orientação de cidadãos como método para otimizar decisões públicas por meio da técnica nudges. *Rev. Bras. Polít. Públicas*, Brasília, v.8, nº2. 2018. Disponível em: <https://publicacoes.uniceub.br/RBPP/article/view/5314>. Acesso em 09 Fev 2023.

SOLOVE, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

SOLTANI, Ashkan; CANTY, Shannon; MAYO, Quentin; THOMAS, Lauren; HOOFNAGLE, Chris J. Flash Cookies and Privacy. *In: AAAI SPRING SYMPOSIUM SERIES*. Palo Alto, California, 2010. p. 158-163. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1446862. Acesso em 09 Fev 2023.

SOUZA, Joyce. Inteligência artificial, algoritmos preditivos e o avanço do colonialismo de dados na saúde pública brasileira. *In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia Literária, 2021. p. 109-127.*

SRNICEK, Nick. *Platform Capitalism*. Cambridge: Polity Press, 2017.

SUMPTER, David. *Dominados pelos números: do Facebook e Google aos algoritmos que controlam nossas vidas*. Tradução de Anna Maria Sotero e Marcello Neto. Rio de Janeiro: Bertrand Brasil, 2019.

SUNSTEIN, Cass R. The Ethics of Nudging. *Yale Journal on Regulation*, v. 32, n. 2, p. 414-450, 2015. Disponível em: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/8225/15_32YaleJonReg413_2015_.pdf?sequence=2&isAllowed=y. Acesso em: 25 nov. 2021.

SZAFIR, Dora; MARKS, Hillary. Consumidores hipervulnerables: ¿necesidad de mayor protección? *Revista de Direito do Consumidor*, São Paulo, v. 31, n. 139, p. 51-72, jan./fev. 2022.

TARTUCE, Flávio. *Manual de Direito Civil*. 11. ed., rev., atual. e ampl. Rio de Janeiro: Forense. 2021. *E-book*.

THALER, Richard. *Misbehaving: a construção da economia comportamental*. Rio de Janeiro: Intrínseca, 2019.

THALER, Richard H. *Nudge, not sludge*. Science, 2018. Disponível em: <https://science.sciencemag.org/content/361/6401/431.full>. Acesso em 20 dez. 2021.

THALER, Richard H.; SUNSTEIN, Cass R. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New York: Penguin Publishing Group. Edição do Kindle, 2009.

VALENTE, Jonas. Brasil tem 134 milhões de usuários de internet, aponta pesquisa. *Agência Brasil*, 26 maio de 2022. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa>. Acesso em: 8 mar. 2022.

VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, [s.l.], v. 12, n. 2, p. 197-208, 2014. Disponível em: https://www.academia.edu/26648535/Datafication_dataism_and_dataveillance_Big_Data_between_scientific_paradigm_and_ideology. Acesso em 09 Fev 2023

VERBICARO, Dennis. A Construção de um novo modelo de cidadania participativa do consumidor a partir da Política Nacional das Relações de Consumo. *Revista de Direito do Consumidor*. vol 110/2017. p. 311 – 339. Mar – Abr. 2017.

VERBICARO, Dennis. Resgatando a importância da transação coletiva de consumo no Brasil. *Revista Jurídica UNICURITIBA*. Vol. 03, nº. 48. Curitiba. 2017. p. 94-117. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Rev-Juridica_UNICURITIBA_n.48.05.pdf. Acesso em 23 Jun de 2021. p. 98-99.

VERBICARO, Dennis; CAÇAPIETRA, Ricardo. A economia comportamental no desenho de políticas públicas de consumo através das Nudges. *Revista de Direito do Consumidor*. vol. 133. ano 30. p. 385-411. São Paulo: Ed. RT, jan./fev. 2021

VERBICARO, Dennis; CALANDRINI, Jorge. Nudges na proteção de dados pessoais no ciberespaço: um empurrão para uma decisão racional do consumidor. *Revista de Direito do Consumidor*. Vol. 142. Ano 31. p. 185-214. São Paulo: Ed. RT, jul./ago. 2022,

VERBICARO, Dennis; CALANDRINI, Jorge. A proteção da confiança do consumidor e a base do legítimo interesse na Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). *Revista de Direito do Consumidor*, São Paulo, v. 31, n. 139, p. 73-99, jan./fev. 2022.

VERBICARO, Dennis; MARANHÃO, Ney; CALANDRINI, Jorge. O impacto do capitalismo de plataforma no agravamento da vulnerabilidade algorítmica do consumidor e do trabalhador. *Revista de Direito do Trabalho*. Vol. 223. P. 277-305. Maio- Jun. 2022.

VERBICARO, Dennis; RODRIGUES, Lays Soares dos Santos. Reflexões sobre o consumo na hipermodernidade: o diagnóstico de uma sociedade confessional. *Revista Direito em Debate*, [s.l.], v. 26, n. 48, p. 342-363, jul./dez. 2017. Disponível em: <https://www.revistas.unijui.edu.br/index.php/revistadireitoemdebate/article/view/6836>. Acesso em: 15 mar. 2022.

VERBICARO, Dennis; RODRIGUES, Lays; ATAÍDE, Camille. Desvendando a vulnerabilidade comportamental do consumidor: uma análise jurídico-psicológica do assédio de consumo. *Revista de Direito do Consumidor*, São Paulo, v. 27, n. 119, p. 349-384, set./out. 2018.

VICENTE, João Paulo. Decisão histórica do STF estabelece proteção de dados pessoais como direito fundamental. *Dadocracia by Data Privacy Brasil*, 30 mar. 2021. *Podcast* [5m 57s]. Disponível em: <https://dataprivacy.com.br/dadocracia-episodio-49-os-primeiros-processos-com-base-na-lgpd/>. Acesso em: 23 ago. 2022.

VITORIO, Tamires. Facebook fica mais perto de 3 bilhões de usuários ativos e receita cresce em 2020. *EXAME*, São Paulo, 28 jan. 2021. Disponível em: <https://exame.com/invest/facebook-fica-mais-perto-de-3-bilhoes-de-usuarios-ativos-e-receita-cresce-em-2020/amp/>. Acesso em: 30 set. 2021.

SUSTEIN, Cass R. The Ethics of Nudging. *Yale Journal on Regulation*. Vol. 32, 2015, p. 417. Disponível em: [The Ethics of Nudging \(yale.edu\)](https://www.yale.edu/ethicsofnudging/). Acesso em 22 dez. 2021.

WAKEFIELD, Jane. Apple x Facebook: a nova ferramenta do Iphone que acirra disputa das gigantes da tecnologia. *BBC News Brasil*, 27 abr. 2021. Disponível em: <https://www.bbc.com/portuguese/geral-56905209>. Acesso em: 16 dez. 2022.

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. *Harvard Law Review*, v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em: <http://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 22 jan. 2022.

WONG, Richmond Y; MULLIGAN, Deirdre K. *Bringing Design to the Privacy Table*. Through the Lens of HCI. In CHI Conference on Human Factors in Computing Systems Proceedings (CHI 2019), May 4–9, 2019, Glasgow, ACM, New York, NY, USA, 17 pages. Disponível em: <https://dl.acm.org/doi/pdf/10.1145/3290605.3300492>. Acesso em 08 de fev de 2022.

WEINGARTEN, Celia. El valor económico de la confianza para empresas y consumidores. *Revista de Direito do Consumidor*, São Paulo, n. 33, p. 33-50, jan./mar. 2000.

WEISEC, Karen. A Amazon sabe quem você é e do que gosta. E ganha bilhões de dólares com isso. *Gazeta do Povo*, 9 fev. 2019. Disponível em: <https://www.gazetadopovo.com.br/economia/a-amazon-sabe-quem-voce-e-e-do-que-voce-gosta-e-ganha-bilhoes-de-dolares-com-isso-bchtf7mvg2dr7nvxtmxkk45gb/#:~:text=O%20neg%C3%B3cio%20de%20publicidade%20da%20Amazon%20vale%20cerca,aparecer%20perto%20de%20resultados%20de%20busca%20de%20produtos>. Acesso em: 19 mar. 2022.

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

ZANELLATO, Marco Antonio. Condutas ilícitas na sociedade digital. *Revista de Direito do Consumidor*, São Paulo, n. 44, p. 206-261, out./dez. 2002.

ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, [s.l.], p. 75-89, 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754. Acesso em: 19 mar. 2022.

ZUBOFF, Shoshana. *A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder*. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.