

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Programa de Pós-graduação em Direito

Leide Jane Macedo da Silva

DATA BROKERS E A COMERCIALIZAÇÃO DE DADOS PESSOAIS:
estratégias empresariais e desafios regulatórios

Belo Horizonte/MG

2025

Leide Jane Macedo da Silva

DATA BROKERS E A COMERCIALIZAÇÃO DE DADOS PESSOAIS:
estratégias empresariais e desafios regulatórios

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para a obtenção do título de Mestra em Direito.

Orientador: Eduardo Goulart Pimenta

Área de concentração: Função Social e econômica das Instituições jurídicas

Belo Horizonte/MG

2025

FICHA CATALOGRÁFICA

Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

S586d	Silva, Leide Jane Macedo da <i>Data brokers</i> e a comercialização de dados pessoais: estratégias empresariais e desafios regulatórios / Leide Jane Macedo da Silva. Belo Horizonte, 2025. 133 f. Orientador: Eduardo Goulart Pimenta Dissertação (Mestrado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito 1. Brasil. Lei geral de proteção de dados (2018). 2. Proteção de dados pessoais - Legislação - Brasil. 3. Dados pessoais - Comércio. 4. Direito à privacidade. 5. Regulamentação. 6. Economia digital. 7. Segurança de dados. I. Brandão, Cláudio Roberto Cintra Bezerra. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito. III. Título. SIB PUC MINAS CDU: 342.721
-------	--

Ficha catalográfica elaborada por Fabiana Marques de Souza e Silva - CRB 6/2086

Leide Jane Macedo da Silva

***DATA BROKERS E A COMERCIALIZAÇÃO DE DADOS PESSOAIS: estratégias
empresariais e desafios regulatórios***

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica de Minas Gerais, como requisito parcial para a obtenção do título de Mestra em Direito.

Área de concentração: Função Social e Função Econômica das Instituições Jurídicas

Prof. Dr. Eduardo Goulart Pimenta - PUC Minas - Orientador

Prof. Dr. Rodrigo Almeida Magalhães - PUC Minas - Banca Examinadora

Prof. Dr. Ivan Guimarães Pompeu - UNA - Banca Examinadora

Belo Horizonte, 30 de junho de 2025.

*"O modo como você reúne, administra e usa a informação
determina se vencerá ou perderá".*

Bill Gates

AGRADECIMENTO

Alcançar este momento representa a concretização de um sonho e um marco significativo em uma trajetória repleta de aprendizados e desafios superados. É com profunda alegria que compartilho estas conquistas, que são fruto do apoio e do amor incondicional de pessoas extraordinárias que estiveram ao meu lado ao longo de todo este percurso.

Primeiramente, dedico esta realização aos meus familiares, que foram minha base sólida, oferecendo força e apoio inabalável em cada passo dado. A presença de cada um de vocês, especialmente minhas filhas e meu marido, foi fundamental para que eu pudesse atravessar todas as etapas dessa jornada. Sem dúvida, a família é o alicerce que sustenta nossos maiores sonhos e nos dá coragem para enfrentarmos os obstáculos.

Aos meus amigos, que compartilharam a vida e a caminhada comigo, meu mais sincero agradecimento. Em especial, à Luciana Castro Bastos, que sempre me motivou e me incentivou a buscar essa conquista. Vocês estiveram presentes tanto nos momentos de incerteza quanto nas celebrações, oferecendo luz e conforto quando os dias se tornavam mais difíceis.

Aos meus professores, minha eterna gratidão. Suas lições, orientações e apoio constante foram verdadeiros pilares que me guiaram ao longo desta caminhada. Em especial, ao meu orientador, Dr. Eduardo Goulart Pimenta, cujo vasto conhecimento, apoio e dedicação profissional foram fundamentais para o meu desenvolvimento e crescimento acadêmico. Ao professor Dr. Rodrigo Almeida Magalhães, um exemplo admirável de competência, profissionalismo e sensibilidade, meu agradecimento sincero por sua generosidade, sabedoria e apoio nos momentos mais cruciais. E ao professor Dr. Dimas Silva, cuja entrada no fim deste semestre trouxe contribuições significativas, agregando novas perspectivas e insights valiosos à minha formação.

Cada um de vocês, com seu comprometimento e generosidade, não só abriu portas para novos saberes, mas também ampliou minha visão de mundo, transformando a forma como percebo o conhecimento e os desafios da vida. O impacto de seu ensino vai além deste trabalho; ele me preparou para tudo o que está por vir.

A todos que, de alguma forma, contribuíram para a realização deste trabalho, meu mais sincero agradecimento. Cada palavra de incentivo, cada gesto de apoio, cada olhar compreensivo foi como uma estrela que iluminou meu caminho, tornando esta jornada ainda mais significativa e inesquecível.

Com imensa gratidão, dedico esta conquista a todos vocês, que foram fundamentais neste capítulo especial da minha vida. Que nossa trajetória sirva de inspiração, lembrando-nos de que grandes realizações são sempre alcançadas com o apoio de pessoas que acreditam em nosso potencial e estão ao nosso lado, nos fortalecendo a cada passo.

Agora, com o coração cheio de gratidão, me preparo para a próxima etapa que me aguarda!

Leide Jane Macedo da Silva

“Nada na vida deve ser temido, somente compreendido. Agora é hora de entender mais, para que possamos temer menos.”

Marie Curie

RESUMO

A digitalização crescente da sociedade tem transformado profundamente a forma como as empresas coletam, processam e utilizam dados pessoais, configurando um mercado global de dados. Os *data brokers*, ou corretores de dados, desempenham papel central nesse cenário ao intermediar a coleta e comercialização de informações pessoais, gerando perfis detalhados dos consumidores. Essa prática, embora economicamente significativa, levanta preocupações sobre a privacidade, a transparência e a conformidade com as regulamentações de proteção de dados, como a LGPD e o GDPR. O estudo visa analisar os desafios regulatórios enfrentados pelos *data brokers*, identificar lacunas nas regulamentações atuais e avaliar o impacto dessas práticas na privacidade dos consumidores e na competitividade das empresas. Utilizando uma abordagem qualitativa, a pesquisa busca oferecer uma compreensão crítica das implicações econômicas, sociais e legais desse mercado, propondo soluções para uma regulação mais ética e transparente.

Palavras-chaves: Data brokers, proteção de dados pessoais, LGPD, GDPR, privacidade, regulamentação, transparência, economia digital, mercado de dados, inovação e empresas.

ABSTRACT

The growing digitalization of society has deeply transformed how companies collect, process, and use personal data, creating a global data market. Data brokers play a central role in this scenario by mediating the collection and commercialization of personal information, creating detailed consumer profiles. Although economically significant, this practice raises concerns about privacy, transparency, and compliance with data protection regulations like the LGPD and GDPR. This study aims to analyze the regulatory challenges faced by data brokers, identify gaps in current regulations, and assess the impact of these practices on consumer privacy and business competitiveness. Using a qualitative approach, the research seeks to provide a critical understanding of the economic, social, and legal implications of this market, proposing solutions for more ethical and transparent regulation.

Keywords: Data brokers, personal data protection, LGPD, GDPR, privacy, regulation, transparency, digital economy, data market, innovation, businesses.

LISTA DE ABREVIATURAS E SIGLAS

4 Vs	Volume, Velocidade, Variedade e Veracidade
AEPD	Agência Espanhola de Proteção de Dados
ANPD	Autoridade Nacional de Proteção de Dados
CCPA	California Consumer Privacy Act - Lei de Privacidade do Consumidor da Califórnia
CDC	Código de Defesa do Consumidor
CDO	Chief Data Officer
CF	Constituição Federal
CIPPIC	Clínica Canadense de Política e Interesse Público da Internet
CNPD	Comissão Nacional de Proteção de Dados de Portugal
CSPs	<i>Content Service Providers</i> - Consumidores e provedores de serviços e conteúdo
DPIA	Avaliação de Impacto sobre a Proteção de Dados
EC	Emenda Constitucional
FTC	Federal Trade Commission - Comissão Federal de Comércio
GDPR	Regulamento Geral de Proteção de Dados
IA	Inteligência Artificial
ICO	Information Commissioner Office
IDEC	Instituto Brasileiro de Defesa do Consumidor
IoT	Internet das Coisas
LGPD	Lei Geral de Proteção de Dados Pessoais
LIA	Teste de Legítimo Interesse
MPDFT	Ministério Público do Distrito Federal e Territórios
PDBs	<i>Personal Data brokers</i>
PIAs	Avaliações de impacto sobre a privacidade
STJ	Superior Tribunal de Justiça
TFH	Tools for Humanity

SUMÁRIO

1 INTRODUÇÃO	13
2 A SOCIEDADE DE DADOS E <i>DATA BROKERS</i>	15
2.1 Sociedade de Dados: Da Datificação ao Império dos Dados	15
2.2 O Capitalismo de Vigilância e os <i>Data Brokers</i>	17
2.3 A Vigilância do Consumidor e o Impacto dos <i>Data brokers</i> na Privacidade: Uma análise de riscos e oportunidades	19
2.3.1 O Impacto dos <i>data brokers</i> na Privacidade	20
2.4 <i>Big Data, Machine Learning</i> e Inteligência Artificial: Ferramentas dos <i>Data brokers</i>	21
2.5. O Papel Econômico e Social dos <i>Data brokers</i> na Economia Digital e Impacto Social	22
2.5.1 O Equilíbrio entre Inovação e Direitos Fundamentais	24
3 A COMERCIALIZAÇÃO DE DADOS PESSOAIS E O MERCADO DE DADOS PESSOAIS	26
3.1 A Comercialização de Dados: Conceito e Modalidades	26
3.1.2 Limites e Condições para a Comercialização de Dados Pessoais e Atuação dos <i>Data Brokers</i>	37
3.1.3 O Caso da <i>Tools For Humanity</i> e a Comercialização de Dados Biométricos	39
3.2 Coleta e Processamento de Dados	42
3.3 Aplicações Comerciais dos Dados Pessoais: Setores e Modelos de Negócios	43
3.3.1 Interseção entre Direito e economia	45
3.4 A Valorização dos Dados Pessoais no Mercado Global: Aplicação do Setor empresarial	47
3.4.1 Riscos e Benefícios da Comercialização de Dados	48
3.4.2 Reflexões sobre os Riscos da Comercialização de Dados Pessoais	49
3.4.4 Desafios e Necessidade de uma Regulação Eficaz	51
3.5 A Fragmentação e o Mercado Global de Dados: O Papel das Empresas Multinacionais	53
4 ASPECTOS LEGAIS E DESAFIOS REGULATÓRIOS	55
4.1 A Evolução das Normativas de Proteção de Dados	55
4.1.1. Regulamentação no Brasil	55
4.1.2 GDPR (<i>General Data Protection Regulation</i>)	59
4.1.3 CCPA (<i>California Consumer Privacy Act</i>)	62
4.2 Análise Comparativa das Normativas de Proteção de Dados	64
4.3 O Papel dos <i>Data brokers</i> nas Normativas de Proteção de Dados	67
4.4 A Conformidade dos Corretores de Dados com a Lei Geral de Proteção de Dados Pessoais	68
4.4.1 O Problema das Bases Legais para o Tratamento de Dados	68
4.5 Os Deveres Aplicáveis aos Corretores de Dados e o Princípio da Boa-Fé ..	71
4.6 O Tratamento Excessivo de Dados e a Proteção dos Direitos Fundamentais	71
4.7 Desafios Regulatórios e Compliance	72
4.7.1 Serasa Experian x MPDFT – Suspensão da Venda de Dados Pessoais e a Importância de Compreender a Atividade dos <i>Data brokers</i> na Economia de Dados	72

4.7.2 A Proteção de Dados Pessoais e a Responsabilidade no Contexto do Credit Scoring	74
4.8 Implementação de Compliance e a Governança no Setor Privado	77
4.8.1 Riscos Legais e Penalidades no Comércio de Dados Pessoais	79
4.9 Desafios Éticos e Sociais na Comercialização de Dados Pessoais	80
4.9.1 Ética Corporativa e Responsabilidade Social	81
4.9.2. Desafios Éticos da Personalização de Serviços e Preços	82
4.10 O Impacto Social da Monopolização de Dados	84
5 IMPLICAÇÕES ECONÔMICAS E EMPRESARIAIS	86
5.1 Empresa e a Economia	86
5.2 A Empresa no Direito Privado	90
5.3 Direito, Empresa e Eficiência	91
5.4 Estrutura da Empresa na Era Digital	95
5.5 O Valor Econômico dos Dados Pessoais: Ativos, Oportunidades e Riscos	99
5.6 Inovação, Competitividade e os Riscos da Dependência de Dados Pessoais	100
5.7 Implicações Regulatórias no Mercado de Dados: Inovação, Competitividade e Modelos de Negócio	103
5.7.1 O Modelo de Tarifa de Duas Partes e Seu Impacto no Excedente do Consumidor e no Setor Empresarial	104
5.7.1.1 Desafios Estratégicos e Concorrenciais Criados pelos PDBs	108
5.7.1.2 Regulação e Sustentabilidade no Mercado de Dados Pessoais	109
5.7.1.3 A Dinâmica Econômica dos Dados Pessoais e os Desafios para as Empresas	109
6 ESTRATÉGIAS EMPRESARIAIS: EQUILÍBRIO ENTRE INOVAÇÃO E ECONOMIA E MERCADO ÉTICO DE DADOS E A PROTEÇÃO DE DADOS	111
6.1 Privacy by Design no contexto da Lei Geral de Proteção de Dados	111
6.2 Integrando Privacy by Design nas Estratégias Empresariais	114
6.3 Privacy by Design e Data Brokers	115
6.4 Diretrizes para a Melhoria das Práticas de Coleta e Uso de Dados Pessoais pelas Empresas	117
6.5 Fortalecimento das Políticas Regulatórias e Mecanismos de Fiscalização	119
6.6 Educação e Conscientização no Uso de Dados	121
7 CONCLUSÃO	124
REFERÊNCIAS	129

1 INTRODUÇÃO

A crescente digitalização da sociedade contemporânea tem impulsionado uma transformação radical na forma como as empresas coletam, processam e utilizam dados pessoais. Esse fenômeno, conhecido como a "datificação" da sociedade, coloca os dados como um ativo estratégico de grande valor na economia digital. Nesse novo cenário, os *data brokers* (corretores de dados) desempenham um papel central, atuando como intermediários especializados na coleta, organização e comercialização de informações pessoais dos consumidores.

Esses dados, que variam desde informações básicas, como contatos e preferências de consumo, até aspectos mais íntimos, como comportamentos online e dados sensíveis, são transformados em perfis detalhados, revendidos para empresas de setores diversos como marketing, finanças, saúde e segurança. Com isso, tem-se a formação de um mercado global de dados, que se expande rapidamente, impactando diretamente as estratégias de negócios e decisões de consumo.

Entretanto, a operação dos *data brokers* é frequentemente invisível e opaca, o que levanta sérias preocupações sobre a transparência e o impacto na privacidade dos indivíduos. A Comissão Federal de Comércio dos Estados Unidos (FTC), ao investigar as práticas dos *data brokers*, destacou a falta de transparência e a necessidade de maior responsabilidade na coleta e no uso desses dados. Muitos consumidores não sabem a extensão das informações que estão sendo coletadas sobre eles nem como essas informações são utilizadas, seja para segmentação publicitária, decisões automatizadas de crédito ou até para práticas de controle comportamental. A afirmação "*Você pode não saber quem são os corretores de dados, mas eles conhecem você*", feita pela Avast em 2021, resume bem o dilema central desse cenário: a invisibilidade das práticas de coleta e comercialização de dados, e a falta de controle dos consumidores sobre suas próprias informações.

Esse mercado global de dados está em plena expansão, e a implementação de regulamentações como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia impõe desafios substanciais aos *data brokers*, que precisam se adaptar a novas normas de transparência, consentimento e proteção de dados. Nesse contexto, a análise crítica das práticas dos *data brokers* torna-se essencial não apenas para entender o impacto econômico da comercialização de dados, mas também para avaliar os riscos à

privacidade e os desafios relacionados à conformidade com as normas de proteção de dados.

A crescente importância da comercialização de dados, associada a práticas cada vez mais complexas, reforça a necessidade urgente de regulamentação. Leis como a Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia representam avanços significativos para enfrentar os desafios da privacidade digital. Contudo, os *data brokers*, como intermediários dessa nova economia, estão cada vez mais expostos às complexidades dessas regulamentações, exigindo adaptação constante às novas normas de transparência, consentimento e proteção de dados.

Apesar da importância econômica que os *data brokers* possuem na economia digital, sua operação levanta sérias questões éticas e legais. A ausência de regulamentação clara, capaz de garantir a proteção dos direitos dos consumidores, ameaça a confiança e a privacidade dos indivíduos. O mercado de dados, com sua crescente complexidade e opacidade, desafia os conceitos de consentimento informado e controle dos dados pessoais, colocando em risco a confiança do consumidor e a manutenção de sua privacidade. Esse cenário evidencia a necessidade de uma regulação robusta, ética e eficaz.

Diante do contexto, o objetivo deste trabalho é analisar as implicações econômicas, sociais e regulatórias do mercado de dados pessoais intermediado pelos *data brokers*. A pesquisa se concentrará em três questões centrais: a) quais são os desafios regulatórios enfrentados pelos *data brokers* no cenário atual?; b) como as lacunas regulatórias podem ser preenchidas para garantir um mercado mais ético e transparente?; e c) qual o impacto dessas práticas na proteção dos direitos dos consumidores e na competitividade das empresas? Além disso, será discutido como equilibrar inovação tecnológica com a proteção de direitos fundamentais, utilizando dados pessoais como ativos estratégicos para as empresas.

A metodologia adotada será qualitativa, baseada em análise documental detalhada, estudos de caso específicos e julgados relevantes sobre o tema, bem como a revisão bibliográfica sobre regulamentos nacionais e internacionais, incluindo como principais as conclusões da FTC, da LGPD e do GDPR. A pesquisa também envolverá uma comparação entre as abordagens regulatórias do Brasil, da União Europeia e dos Estados Unidos, com o objetivo de oferecer uma contribuição significativa para a

formulação de políticas públicas que promovam um mercado de dados mais ético e transparente, em conformidade com os direitos dos consumidores.

Em última análise, o estudo busca fornecer uma compreensão crítica sobre o mercado de dados pessoais e as implicações dessa prática no direito empresarial. A pesquisa pretende ainda apoiar a construção de regulamentações que promovam práticas empresariais responsáveis, equilibrando inovação com proteção dos direitos dos consumidores e criando um ambiente digital mais transparente e ético, pretendendo, assim, enriquecer o debate acadêmico e apoiar a construção de regulamentações que assegurem a proteção dos dados pessoais, ao mesmo tempo em que promovem práticas empresariais responsáveis e equilibradas.

2 A SOCIEDADE DE DADOS E *DATA BROKERS*

2.1 Sociedade de Dados: Da Datificação ao Império dos Dados

A sociedade contemporânea passou por uma transformação profunda, impulsionada pela revolução digital. O advento da "sociedade de dados", caracterizada pela coleta, análise e comercialização de grandes volumes de dados pessoais, está reformulando não apenas a interação entre pessoas, mas também as práticas empresariais e a estrutura econômica global. No centro dessa mudança está o conceito de "datificação", que descreve o processo de converter comportamentos, atividades cotidianas e até mesmo emoções humanas em dados digitais. Esses dados, uma vez coletados, são analisados e transformados em um novo tipo de mercadoria: a informação, que passou a ser considerada o "novo petróleo" (Zuboff, 2019), uma mercadoria valiosa que não só alimenta o comércio, mas também influencia decisões e antecipa comportamentos.

No centro dessa revolução encontram-se os *Data brokers*, ou Corretores de Dados, que atuam como intermediários especializados na coleta, análise e comercialização de vastos volumes de dados pessoais. Esses agentes agregam informações de diversas fontes, como registros públicos, transações financeiras, dados de redes sociais e dispositivos conectados pela Internet das Coisas (IoT). Segundo a definição da FTC, *data brokers* são empresas que "reúnem dados sobre consumidores de diversas fontes e vendem esses dados a outras companhias" (FEDERAL TRADE COMMISSION, 2014).

A origem dos *data brokers* está ligada às práticas de marketing e pesquisa de mercado das décadas de 1980 e 1990, intensificadas pelo avanço da computação e pela digitalização da informação. O salto da era analógica para a digital foi um ponto de inflexão decisivo na forma como as sociedades armazenam e processam informações. Antes da digitalização, os dados estavam restritos a suportes físicos, como papéis e arquivos, e eram acessados de maneira lenta e limitada. No entanto, com a explosão da digitalização nas últimas décadas, a quantidade de dados gerados e processados passou a crescer de forma exponencial. Em 2013, cerca de 98% de todas as informações estavam em formato digital (Mayer-Schönberger e Cukier, 2013).

Essas empresas estruturaram-se como poderosos conglomerados de armazenamento e processamento de dados, operando por meio de sofisticados arranjos de computação em nuvem (Alowairdhi e Ma, 2019). Empresas como Acxiom, Experian (conhecida no Brasil como Serasa Experian), Epsilon e Core Logic se consolidaram como líderes nesse setor (Singer, 2012).

Na economia de hoje, Big Data é um grande negócio. *Data brokers* – empresas que coletam informação pessoal dos consumidores e revendem ou compartilham com outros – são importantes participantes da economia do Big Data. (FEDERAL TRADE COMMISSION, 2014).

O *data brokers* agregam dados de diversas fontes, como transações online, dados de dispositivos conectados pela Internet das Coisas (IoT), informações de redes sociais e muito mais. Usando algoritmos avançados de aprendizado de máquina (*machine learning*), esses *brokers* constroem perfis detalhados de consumidores, que são então comercializados para uma variedade de finalidades — desde campanhas de marketing personalizado até análises de crédito e previsões de comportamento.

Com a capacidade de armazenar e analisar enormes volumes de dados em tempo real, surgiram novas formas de *Big Data*, um conceito que descreve grandes conjuntos de dados que podem ser analisados para gerar insights em tempo recorde. Os 4 Vs do *Big Data* — Volume, Velocidade, Variedade e Veracidade — tornam-se essenciais para entender o impacto desta digitalização em setores como saúde, marketing, segurança e financeiro.

Contudo, esse cenário levanta questões cruciais: a privacidade está sendo protegida? Os indivíduos têm controle sobre seus dados? Embora a comercialização

de dados traga benefícios econômicos, ela também desafia os marcos regulatórios tradicionais, colocando em jogo os direitos fundamentais dos indivíduos (Doneda, 2014). A necessidade de uma legislação robusta e eficaz se torna cada vez mais premente para garantir que o uso de dados pessoais não ultrapasse os limites do consentimento e da ética, bem como seja oportunizado crescimento do mercado e através da inovação.

No entanto, essa evolução não está isenta de riscos. Autores como Bauman (2013) e Rodotà (2016) alertam para a dependência crescente dos dados e as ameaças que ela impõe, como o controle social, a manipulação de comportamentos e até a discriminação algorítmica. A transição digital exige, portanto, uma reflexão mais profunda sobre como o Direito pode acompanhar a inovação, equilibrando o uso de dados com a proteção dos direitos individuais.

2.2 O Capitalismo de Vigilância e os *Data Brokers*

No livro *"The Age of Surveillance Capitalism"*, a autora Shoshana Zuboff (2018) apresenta uma análise crítica sobre o fenômeno do capitalismo de vigilância, caracterizando-o como um marco fundamental para a defesa digital individual. A autora detalha o processo de coleta e mineração de dados, ilustrando como nossas ações e comportamentos são moldados por práticas comerciais, além de discutir as implicações dessa dinâmica para o Estado de Direito. Esse fenômeno emerge do que Zuboff descreve como um "mercado de comportamentos futuros", onde dados pessoais são comprados e vendidos com o objetivo de desenvolver produtos e serviços que visam influenciar as escolhas dos consumidores.

A coleta de dados pessoais não só influencia comportamentos, mas também redefine as dinâmicas de poder e controle social. A autora alerta que o capitalismo de vigilância, fundamentado na coleta e comercialização de dados, gera uma nova configuração econômica que mina a privacidade dos indivíduos e ameaça os direitos humanos.

Para entender melhor a proposta de Zuboff, apresenta-se a definição que a autora elabora sobre a definição de Capitalismo de Vigilância (Zuboff, 2018):

- a) Uma nova configuração econômica que utiliza experiências humanas como matéria-prima para práticas ocultas de extração, previsão e comercialização;
- b) Uma lógica de economia parasitária em que a produção de bens e serviços se submete a uma nova arquitetura global de modificação do comportamento;
- c) Uma transformação do capitalismo caracterizada por concentrações sem precedentes de riqueza, conhecimento e poder na história;
- d) A base da estrutura da economia de vigilância;
- e) Uma ameaça significativa à natureza humana no século XXI, assim como o capitalismo industrial impactou o meio ambiente nos séculos XIX e XX;
- f) A gênese de um novo poder que exerce controle sobre a sociedade, apresentando desafios significativos à democracia;
- g) Um movimento que busca instaurar uma nova coletividade fundamentada na certeza absoluta;
- h) Uma erosão dos direitos humanos que pode ser vista como um golpe elitista, desestabilizando a soberania popular.

Neste contexto, a extração e comercialização das experiências humanas como matéria-prima para prever comportamentos configura uma nova lógica econômica, que, ao buscar modificar as ações dos indivíduos, se torna uma economia parasitária. Nesse modelo, a produção de bens e serviços deixa de ser apenas uma resposta às necessidades dos consumidores, transformando-se em um esforço consciente para moldar suas escolhas e ações. Esse fenômeno implica desafios significativos à democracia, pois resulta em uma concentração inédita de poder e riqueza nas mãos de poucos, prejudicando a autonomia e a privacidade dos indivíduos. As repercussões disso não se restringem apenas ao âmbito econômico, mas se expandem para o campo dos direitos humanos, ameaçando as liberdades fundamentais e a capacidade dos indivíduos de tomar decisões livres em um ambiente cada vez mais controlado.

Essa dinâmica é impulsionada pela crescente sofisticação das tecnologias de coleta de dados, com os *data brokers* desempenhando um papel central na criação de perfis de consumidores, frequentemente sem o conhecimento ou consentimento deles.

2.3 A Vigilância do Consumidor e o Impacto dos *Data brokers* na Privacidade: Uma análise de riscos e oportunidades

A vigilância do consumidor, impulsionada pelos avanços tecnológicos, tem transformado a maneira como as empresas coletam, analisam e utilizam os dados dos indivíduos. O monitoramento da atividade dos consumidores para fins comerciais tem se tornado cada vez mais sofisticado, possibilitando a criação de perfis detalhados, a identificação de padrões comportamentais e a indução de determinadas ações. Embora a coleta de dados pessoais tenha sido uma prática histórica, com o aumento da digitalização das interações entre empresas e consumidores, o processo se tornou muito mais intrusivo, como aponta Schneier (2006).

Schneier (2006) identifica quatro principais fontes históricas de coleta de informações sobre consumidores. A primeira delas refere-se aos dados pessoais armazenados pelas próprias empresas, como pedidos e informações cadastrais, que eventualmente evoluíram para grandes bancos de dados. A segunda fonte vem do marketing direcionado, em que as empresas usavam o correio para enviar propaganda personalizada, inicialmente baseando-se em dados demográficos e informações simples, como assinaturas de revistas. A terceira fonte são as agências de crédito, que coletam informações detalhadas sobre a situação financeira dos consumidores e vendem esses dados para bancos e instituições financeiras, a fim de auxiliar na concessão de crédito. Por fim, a quarta fonte de dados são os registros públicos disponibilizados pelo Estado, como informações de litígios, registros de identidades e outros dados de domínio público.

Com o avanço da era digital, o cenário mudou drasticamente. A redução dos custos de tecnologia de computação e armazenamento de dados possibilitou o acesso a ferramentas de coleta e análise de dados para uma quantidade crescente de empresas. O conceito de Big Data passou a dominar, com as empresas buscando não apenas coletar, mas também analisar e armazenar grandes volumes de dados sobre os consumidores, criando novas dinâmicas comerciais e sociais.

Nesse contexto, surgem os *data brokers*, empresas especializadas na compra e venda de dados pessoais. Segundo Marta Peirano (2019), esses intermediários têm como função reunir informações dispersas sobre indivíduos e criar um perfil único e detalhado de cada pessoa. Eles adquirem dados pessoais de diversas fontes, como

compras realizadas em lojas, informações de redes sociais, dados financeiros e até mesmo de mercados paralelos. O trabalho dos *data brokers* é montar uma base de dados capaz de fornecer informações valiosas para empresas de diferentes setores, desde marketing até análise de risco financeiro.

2.3.1 O Impacto dos *data brokers* na Privacidade

O impacto dessa prática pode ser vasto, pois os dados pessoais são utilizados para segmentar consumidores de maneira minuciosa, e não apenas para direcionar campanhas de marketing, mas também para influenciar decisões importantes, como ofertas de crédito e até mesmo os resultados de eleições. A venda e a análise de dados também podem gerar consequências inesperadas e prejudiciais para os consumidores, como aumento de prêmios de seguros, rejeição de empréstimos e até mesmo discriminação com base em informações que o consumidor não sabe que estão sendo compartilhadas.

Um exemplo concreto desse tipo de coleta de dados são os programas de fidelidade, em que as empresas oferecem descontos e vantagens em troca de informações sobre o comportamento de compra dos consumidores. Embora esses programas possam parecer inofensivos à primeira vista, eles acabam por gerar um perfil completo do consumidor, reunindo dados financeiros, de saúde, comportamento de compra e preferências pessoais. Como no caso de farmácias que coletam dados através de programas de fidelidade e, posteriormente, compartilham essas informações com terceiros, como empresas de plano de saúde e de análise de crédito. Com isso, dados como o histórico de compras de medicamentos podem ser usados para ajustar preços de serviços ou até mesmo para restringir acessos a crédito.

A crescente exposição dos dados pessoais e a comercialização desses dados geram um cenário de vulnerabilidade para os consumidores. A recente implementação da Lei Geral de Proteção de Dados nº 13.709/18 (LGPD) no Brasil é um esforço para estabelecer regras mais rigorosas sobre o tratamento de dados pessoais* e proteger a privacidade dos indivíduos.

De acordo com o Artigo 5º da LGPD, são considerados dados pessoais aquelas informações relacionadas a uma pessoa natural identificada ou identificável, enquanto dados pessoais sensíveis incluem informações sobre origem racial ou étnica, convicção religiosa, opinião política, dados relativos à saúde, vida sexual, entre outros,

quando vinculados a uma pessoa natural. Além disso, o tratamento de dados engloba todas as operações realizadas com dados pessoais, como coleta, armazenamento, modificação, transmissão e eliminação de informações, o que destaca a amplitude e a importância da regulamentação.

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; [...]

X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018).

No entanto, conforme afirmam Frazão (2020) e Doneda (2019), as leis por si só não são suficientes. A fiscalização eficaz e a conscientização pública são fundamentais para garantir que os dados pessoais não sejam utilizados de maneira prejudicial.

Portanto, a proteção da privacidade na era digital não pode ser vista como responsabilidade exclusiva dos reguladores ou das empresas. Ela requer um esforço conjunto entre governos, empresas e consumidores. Reguladores devem implementar e fiscalizar as leis de forma rigorosa; as empresas devem garantir que os dados pessoais sejam tratados de maneira ética e transparente; e os consumidores devem ser educados para compreender o valor de seus dados e as possíveis consequências da sua exposição. Só assim será possível garantir um ambiente digital seguro e respeitador dos direitos fundamentais de privacidade.

2.4 *Big Data*, *Machine Learning* e Inteligência Artificial: Ferramentas dos *Data brokers*

A ascensão dos *data brokers* está intrinsecamente ligada ao uso de tecnologias avançadas, como *Big Data*, *Machine Learning* e Inteligência Artificial (IA). Esses intermediários coletam dados de múltiplas fontes e, por meio de algoritmos sofisticados, criam perfis de consumidores que preveem comportamentos futuros, como decisões de compra, análise de crédito e até mesmo interações sociais.

O Big Data refere-se a grandes volumes de dados que, por sua variedade, velocidade e complexidade, não podem ser processados com as ferramentas tradicionais de análise. Já o *machine learning* permite que os sistemas aprendam padrões a partir desses dados, automatizando previsões e decisões de maneira cada vez mais precisa.

Esse uso de tecnologias emergentes permite que os *data brokers* construam perfis detalhados, criando uma verdadeira economia de comportamento. No entanto, essa dinâmica também abre caminho para riscos consideráveis, como discriminação algorítmica, onde decisões podem ser baseadas em padrões discriminatórios ou preconceituosos, ou ainda manipulação de preferências e escolhas sem o consentimento dos consumidores. A opacidade desses processos é um dos maiores desafios, já que muitas vezes os indivíduos sequer têm conhecimento de como seus dados estão sendo coletados e utilizados.

2.5. O Papel Econômico e Social dos *Data brokers* na Economia Digital e Impacto Social

Os *data brokers* desempenham um papel central na economia digital ao atuar como intermediários entre os geradores de dados (os consumidores) e os compradores desses dados (empresas de marketing, seguradoras, bancos, entre outras). Através da combinação de dados *online* e *offline*, esses intermediários conseguem criar perfis detalhados que não só otimizam campanhas publicitárias, mas também são usados para avaliar riscos financeiros e até mesmo prever comportamentos futuros, o que confere um poder considerável às empresas que controlam essas informações.

Esse modelo econômico, no entanto, levanta importantes questões sobre desigualdade e controle social. A comercialização de dados pessoais frequentemente ocorre sem o conhecimento ou consentimento dos indivíduos, colocando em risco a autonomia e a privacidade. A falta de transparência e a manipulação das escolhas dos consumidores, baseadas em perfis muitas vezes imprecisos ou discriminatórios, podem gerar uma série de impactos sociais, desde a perda de liberdade individual até a criação de um sistema de controle social sem precedentes.

Os *data brokers* raramente interagem diretamente com os consumidores, o que contribui para a invisibilidade de suas práticas. Segundo a FTC, essas empresas

utilizam fontes variadas – comerciais, governamentais e públicas – para coletar dados crus e inferências derivadas. Elas combinam informações obtidas *online* e *offline*, criando perfis detalhados que incluem hábitos de compra, histórico financeiro e até mesmo características sensíveis.

A pesquisa da FTC revelou práticas preocupantes, como o armazenamento de dados pessoais de praticamente todos os consumidores norte-americanos e o uso desses dados para criar modelos complexos que predizem comportamentos. Além disso, a troca e comercialização de informações entre diferentes camadas de data brokers aumentam a complexidade do setor, dificultando a supervisão regulatória.

A indústria dos *data brokers* ocupa um papel central na economia baseada em dados, oferecendo informações pessoais para diversos fins, como marketing, mitigação de riscos e localização de indivíduos. Contudo, a atuação dessas empresas é caracterizada por uma preocupante falta de transparência. O relatório da Federal Trade Commission (FTC) de 2014, "*Data brokers: a call for transparency and accountability*", aponta que a coleta e o uso de dados ocorrem, na maioria das vezes, sem o conhecimento ou consentimento dos consumidores afetados, refletindo a complexidade e a opacidade do mercado de dados.

O consentimento, conceitualmente, é a pedra angular sobre a qual repousa a gestão ética e legal de informações pessoais em um mundo cada vez mais conectado. Essencialmente, representa a expressão voluntária de um indivíduo concordando com a coleta, processamento e uso de seus dados pessoais. Essa noção básica de escolha individual deve ser a base de muitas leis de proteção de dados em todo o mundo. É importante ressaltar que os dados pessoais podem variar de públicos a sigilosos. Alguns dados, como registros de propriedade imobiliária, são públicos e de acesso geral, enquanto informações médicas, orientação sexual, crenças religiosas e dados financeiros são consideradas sensíveis e recebem maior proteção sob as leis de proteção de dados (COSTA; COSTA, 2024, p. 41).

O artigo 5 da LGPD conceitua o consentimento:

Art. 5º. Para os fins desta Lei, considera-se:

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. (Brasil, 2018).

No entanto, embora o consentimento seja vital, sua implementação prática enfrenta desafios significativos. Um desses desafios é o consentimento informado.

Com frequência, os titulares de dados são apresentados a longos e complexos termos de serviço ou políticas de privacidade, que raramente são lidos integralmente. Isso levanta questões sobre a eficácia do consentimento quando os indivíduos não compreendem plenamente as implicações de suas escolhas.

O consentimento é, portanto, uma peça fundamental nas leis de proteção de dados, exigindo que as organizações obtenham o consentimento informado, específico e voluntário dos titulares antes de coletar, processar ou compartilhar seus dados pessoais. No entanto, o consentimento não é a única base legal para o processamento de dados, já que a lei pode permitir o processamento sem consentimento em situações específicas, como cumprimento de obrigações legais ou proteção de interesses vitais e funções de interesse público.

Do ponto de vista tecnológico, a gestão do consentimento também é complexa. Sistemas e processos precisam ser implementados para rastrear e gerenciar as preferências de consentimento dos titulares de dados de maneira eficaz (COSTA; COSTA, 2024, p. 41).

2.5.1 O Equilíbrio entre Inovação e Direitos Fundamentais

À medida que os *data brokers* se tornam protagonistas no mercado de dados, surgem desafios jurídicos cada vez mais complexos. A crescente dependência de dados exige uma reflexão urgente sobre os limites da inovação tecnológica. A legislação precisa acompanhar as mudanças rápidas e assegurar que as práticas de coleta e comercialização de dados pessoais estejam em conformidade com os princípios de transparência, necessidade e consentimento. O equilíbrio entre inovação e direitos fundamentais é essencial para garantir que a sociedade digital não se transforme em um espaço de controle absoluto, ameaçando a liberdade e a dignidade humana.

Além disso, a comercialização de dados pessoais frequentemente ocorre sem que os indivíduos saibam como suas informações estão sendo utilizadas. Em um mundo onde os dados alimentam algoritmos que podem prever e até mesmo influenciar comportamentos, a falta de transparência se torna uma questão fundamental.

A implementação da LGPD e a observância de legislações comparadas é um passo importante para regular o uso de dados pessoais e assegurar a privacidade dos

indivíduos. Porém, a efetiva aplicação da lei exige fiscalização rigorosa e adaptação contínua às novas tecnologias. O que ocorre, muitas vezes, é que a regulação não acompanha a velocidade das inovações tecnológicas, criando um cenário de vulnerabilidade para os consumidores e abrindo margem para abusos por parte das empresas.

A enorme quantidade de dados gerada e a falta de transparência com que os *data brokers* operam indicam a necessidade urgente de mecanismos de fiscalização robustos. O Direito deve agir como um mediador entre o impulso pela inovação e o respeito aos direitos fundamentais. Como alertam Zuboff (2018) e Frazão (2020), um modelo de economia baseado em dados não pode ignorar a importância de equilibrar o avanço tecnológico com a proteção da dignidade humana.

A governança de dados deve, portanto, ser um tema central nas políticas públicas, garantindo que as empresas não apenas aproveitem os dados para incrementar suas estratégias, mas também respeitem os direitos de privacidade e autonomia dos indivíduos. O sistema jurídico precisa estar preparado para lidar com o impacto que os *data brokers* têm na sociedade, especialmente quando a coleta e comercialização de dados pessoais acontecem sem o devido consentimento.

O risco de um futuro no qual os indivíduos perderiam total controle sobre suas informações pessoais é real e deve ser enfrentado com medidas regulatórias claras e eficazes. Caso contrário, podemos estar diante de uma sociedade de controle, onde os dados são utilizados para manipular comportamentos e decisões, colocando em risco a liberdade individual e a dignidade humana.

A sociedade de dados, impulsionada pela atuação dos *data brokers*, está transformando profundamente a economia digital e a interação social. Embora as inovações tecnológicas tragam benefícios econômicos, elas também impõem desafios significativos em termos de privacidade, controle social e desigualdade. A LGPD e outras legislações de proteção de dados representam passos importantes para regular o uso de dados pessoais, mas a verdadeira proteção só será alcançada com a fiscalização eficaz e a conscientização pública. O equilíbrio entre inovação e respeito aos direitos individuais será fundamental para garantir uma sociedade digital justa e ética.

3 A COMERCIALIZAÇÃO DE DADOS PESSOAIS E O MERCADO DE DADOS PESSOAIS

3.1 A Comercialização de Dados: Conceito e Modalidades

A comercialização de dados pessoais ocupa posição central nas discussões contemporâneas sobre privacidade, economia digital e regulação de tecnologias. Com o advento da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), o Brasil se alinhou a um movimento global de reconhecimento da importância de proteger os dados como manifestação da dignidade humana e como ativos de altíssimo valor econômico. Este capítulo analisa os aspectos jurídicos, doutrinários e práticos da comercialização de dados pessoais, com base na doutrina brasileira atual e nos parâmetros internacionais, como o GDPR (2016) europeu.

Ao longo das últimas décadas, os dados pessoais emergiram, como insumos estratégicos de altíssimo valor no contexto da economia digital. A crescente coleta e utilização de dados por plataformas digitais como redes sociais, mecanismos de busca, marketplaces e aplicativos diversos revela o surgimento de uma nova engrenagem econômica: o mercado de dados pessoais.

A monetização da informação pessoal reflete o que Shoshana Zuboff (2019) denominou “capitalismo de vigilância”, em que a coleta massiva de dados passa a integrar modelos de negócio baseados na predição comportamental. Nesse cenário, a informação deixa de ser um mero reflexo da vida privada e passa a ser tratada como matéria-prima, objeto de trocas econômicas, publicidade direcionada, e até manipulação social.

Diante dessa realidade, surge uma indagação central: é legítimo comercializar dados pessoais? E, se sim, sob quais limites éticos e jurídicos essa prática pode ser admitida? A resposta a essas perguntas exige confrontar dois vetores fundamentais do ordenamento jurídico: de um lado, a autonomia da vontade (CF, art. 5º, II), que fundamenta a liberdade contratual e a disposição de direitos; de outro, os direitos da personalidade, como a proteção da dignidade da pessoa humana (CF, art. 1º, III), a privacidade (art. 5º, X) e, mais recentemente, a proteção de dados como direito fundamental (art. 5º, LXXIX, incluído pela EC nº 115/2022).

Na prática, muitos usuários já fornecem seus dados em troca de serviços digitais gratuitos, ainda que de forma inconsciente. A ausência de remuneração direta

não elimina o caráter econômico da operação. Por isso, é essencial estabelecer regras claras sobre acesso, finalidade, duração e garantias para o titular dos dados.

A comercialização de dados pessoais pode ser entendida como a transferência onerosa dessas informações entre agentes econômicos, com vistas à obtenção de lucro. Tal prática, embora amplamente difundida, especialmente por *data brokers* e plataformas digitais, gera uma série de questionamentos sobre sua legalidade e compatibilidade com os princípios da proteção de dados e da dignidade da pessoa humana.

a) Formas de Comercialização: Direta e Indireta

A comercialização de dados pode ocorrer de forma direta ou indireta, e é essencial compreender essas distinções para entender as implicações jurídicas e econômicas dessa prática.

1. **Comercialização Direta:** Refere-se à venda ou troca de dados pessoais diretamente para empresas que os utilizam para finalidades comerciais, como marketing, publicidade ou desenvolvimento de produtos. Por exemplo, quando um indivíduo fornece seus dados em troca de um serviço ou produto gratuito, como ocorre em muitas plataformas digitais. Empresas como Meta ou Google praticam essa modalidade ao coletar dados e vendê-los para agências de publicidade para segmentação de anúncios.
2. **Comercialização Indireta:** Ocorre quando os dados pessoais são vendidos ou repassados para intermediários, como *data brokers*, que os agregam e revendem a empresas para análise de mercado, avaliação de risco, entre outros usos. Neste modelo, o titular pode nem sempre ter ciência de que seus dados estão sendo compartilhados com terceiros, o que levanta preocupações sobre a falta de transparência e a opacidade dos processos envolvidos.

A comercialização indireta, em particular, é frequentemente realizada sem o conhecimento explícito do titular dos dados, o que gera discussões sobre a necessidade de regulação mais eficaz para proteger os direitos dos indivíduos. A

LGPD, por exemplo, impõe limites ao compartilhamento de dados com terceiros, exigindo que o consentimento seja claro e revogável (BRASIL, 2018, art. 8º).

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.

Mesmo ao aceitar cookies ou políticas de privacidade, o usuário muitas vezes consente, de forma ampla e sem plena consciência, com o uso comercial de seus dados. Isso evidencia a necessidade de um marco jurídico que assegure o equilíbrio entre exploração econômica e proteção de direitos fundamentais.

Assim, ainda que juridicamente possível em determinadas circunstâncias, a venda de dados pessoais está condicionada a um ambiente jurídico estrito, que busca equilibrar os interesses econômicos com a tutela dos direitos fundamentais dos titulares.

b) Monetização de Dados: Conceito e Modalidades

Conforme Rodrigo Valadão (2025), a monetização de dados difere da comercialização direta. Enquanto esta geralmente envolve cessão onerosa a terceiros, a monetização refere-se à exploração econômica dos dados sem necessariamente transferi-los. Os dados funcionam como insumos estratégicos em modelos de negócio que geram valor por meio de publicidade personalizada, precificação dinâmica, análise comportamental e coleta de metadados.

Essa monetização pode ocorrer de maneira primária, quando há uma relação direta entre o titular dos dados e o agente que os explora economicamente, ou secundária, quando essa exploração ocorre entre controladores ou operadores sem a participação ativa do titular. Este capítulo concentra-se nos modelos de monetização primária, nos quais os titulares têm a possibilidade de obter uma contrapartida econômica, direta ou indireta, pela utilização de seus dados pessoais.

O STJ brasileiro já reconheceu que a oferta de serviços digitais gratuitos mediante uso de dados configura relação de consumo, o que reforça a necessidade de regulação adequada. Um exemplo emblemático é o Recurso Especial nº 1.186.616/MG, julgado em 23/08/2011, sob a relatoria da Ministra Nancy Andrighi. Nesse caso, a Terceira Turma do STJ reafirmou que a exploração comercial da

internet sujeita as relações daí advindas à Lei nº 8.078/90 (Código de Defesa do Consumidor), mesmo que o serviço prestado seja gratuito. O termo "mediante remuneração", contido no art. 3º, § 2º, do CDC, deve ser interpretado de forma ampla, incluindo o ganho indireto do fornecedor, como a coleta de dados pessoais dos usuários.

Outras práticas comuns incluem programas de fidelização, que oferecem benefícios econômicos em troca de dados comportamentais. Modelos como "desconto por dados" são amplamente utilizados nos setores de saúde, seguros e varejo, envolvendo, por exemplo, o uso de *wearables* para redução de mensalidades ou personalização de cupons com base em padrões de consumo.

Essas práticas, embora inovadoras, demandam sólidas bases legais e transparência. Algumas propostas, como o "*Data Dividend*", defendem a redistribuição da riqueza gerada pela exploração de dados, propondo formas de compensação social.

A monetização direta, por sua vez, trata os dados como ativos individuais patrimonializáveis, cuja autorização de uso é remunerada de forma explícita. Nesse modelo, o titular exerce maior controle sobre a negociação de seus dados, recebendo compensações financeiras ou benefícios equivalentes, como créditos, milhas ou *acesso premium*. Aplicativos e plataformas que adotam esse modelo permitem ao usuário escolher quais informações deseja compartilhar e obter retorno proporcional ao valor atribuído a esses dados. Programas de *cashback*, participação em pesquisas remuneradas e venda de dados de navegação ou localização são alguns exemplos práticos.

Valadão destaca que a monetização dos dados envolve arranjos contratuais e tecnológicos que podem beneficiar o titular, mas alerta para os riscos da *comoditização* da privacidade, ao transformar dados pessoais dotados de caráter personalíssimo em simples mercadorias, o que pode implicar na erosão de direitos fundamentais se não houver limites bem definidos.

Modelos inovadores, como as *Personal Data Exchanges (PDEs)*, permitem ao titular gerenciar seus dados por meio de *blockchain* e cofres digitais, assegurando maior transparência e controle. Alternativamente, as cooperativas de dados propõem uma gestão coletiva, baseada em princípios de adesão voluntária, governança democrática e partilha equitativa dos benefícios. Esses arranjos reconfiguram a

informação pessoal como bem comum, em contraposição à lógica centralizadora das grandes plataformas.

Independentemente da modalidade, a monetização deve observar princípios de autodeterminação informativa, transparência e segurança, preservando a dignidade do titular.

Um exemplo prático ilustra essa dinâmica: ao pesquisar “viagem para Brasília” no Google, esse comportamento gera dados que alimentam sistemas de inteligência artificial. Esses dados conectam o usuário a empresas de turismo que, por sua vez, pagam para veicular anúncios personalizados. Essa cadeia de valor, embora legítima, torna-se problemática quando ocorre sem consentimento, compensação ou transparência.

Plataformas como o “*Google Ads*”, que utiliza inteligência artificial para segmentar anúncios com base em nossos dados pessoais (comportamentos online). Quando fazemos uma pesquisa rápida no “Google”, como “viagem para Brasília”, esse comportamento gera um dado interpretado como: “João procura uma viagem para Brasília”. Esse dado alimenta sistemas de inteligência artificial que o conectam com empresas de pacotes turísticos, interessados em oferecer suas ofertas a pessoas como João. Contudo, a exploração desses dados sem o devido controle do titular pode configurar um problema ético e legal.

A Lei Geral de Proteção de Dados (LGPD) oferece diretrizes para a coleta e uso de dados, mas o respeito a tais normas depende da adesão a práticas empresariais éticas, pautadas pela segurança, clareza e consentimento expresso. A rápida evolução tecnológica e os novos modelos de negócio impõem o desafio de atualizar permanentemente os instrumentos normativos, exigindo atuação proativa do legislador e dos órgãos reguladores.

A rapidez das mudanças tecnológicas e a complexidade dos novos modelos de negócio exigem vigilância contínua para garantir o cumprimento das normas e adaptar a legislação à realidade dinâmica do mercado. As empresas devem ser responsabilizadas pela coleta e uso de dados, adotando uma gestão que respeite a privacidade, promova a autodeterminação informativa e evite abusos.

Assim, a regulamentação deve equilibrar os interesses comerciais com a proteção dos direitos fundamentais, respeitando a dignidade humana e promovendo um ambiente digital ético e sustentável. A legislação brasileira, alinhada às normas

internacionais, deve ser dinâmica e capaz de acompanhar o crescimento exponencial da economia de dados, garantindo que os direitos dos indivíduos sejam sempre respeitados. A comercialização e monetização dos dados pessoais devem ocorrer dentro de um regime jurídico que proteja a privacidade, a autodeterminação informativa e a dignidade do titular.

3.1.1 Dados como Propriedade? Entre a Autodeterminação Informativa e a Patrimonialização

No contexto da sociedade da informação, em que os dados pessoais se tornaram insumos estratégicos para a economia digital, ganha força o debate sobre seu possível enquadramento jurídico como formas de propriedade. A crescente valorização econômica dos dados, catalisada pelo modelo de negócios das plataformas digitais, suscita uma indagação fundamental: é juridicamente admissível conceber os dados pessoais como bens patrimoniais disponíveis, ou sua natureza intrinsecamente ligada à personalidade impõe sua regência exclusiva pelos direitos fundamentais?

De um lado, emergem concepções que propõem a patrimonialização dos dados. Para autores como Lawrence Lessig (2004), a atribuição de um regime jurídico proprietário poderia oferecer maior previsibilidade normativa, além de conferir ao titular maior poder de controle e disposição sobre suas informações. Nessa lógica, os dados pessoais seriam dotados de valor econômico e, como tais, passíveis de negociação tal como ocorre com outros direitos da personalidade, como a imagem ou a voz.

No plano jurídico, a privacidade é tradicionalmente compreendida como direito fundamental de cunho existencial, não disponível em termos absolutos. Dados pessoais, enquanto expressão dessa privacidade, carregam uma dimensão sensível e imaterial que impede sua redução a simples mercadorias (GOMES, 2018). Ainda assim, a crescente mercantilização das informações pessoais impulsionou a reflexão sobre a viabilidade de um regime híbrido, capaz de compatibilizar a proteção da personalidade com a realidade econômica da circulação de dados (DURHAM, 2015).

A Lei Geral de Proteção de Dados Pessoais (LGPD) adota uma abordagem que reflete essa tensão. A norma reconhece, no art. 5º, a figura do titular como a

pessoa natural a quem os dados se referem, e define os dados pessoais como informações relacionadas a pessoa natural identificada ou identificável.

Em uma relação envolvendo dados pessoais, de um lado está o titular desses dados e, do outro, os agentes de tratamento dos dados, controlador e operador de dados. A titularidade dos dados pessoais é definida pelo art. 5º, V, da LGPD, e pressupõe o conhecimento do significado de dados pessoais, por sua vez constante do art. 5º, I, nos seguintes termos:

Art. 5º Para os fins desta Lei, considera-se:

I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

[...]

V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Sob essa perspectiva, a autodeterminação informativa emerge como princípio estruturante da proteção de dados pessoais. Ela garante ao titular o controle sobre o uso de suas informações, conforme reconhecido pela Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018 –, que não atribui aos dados uma natureza de propriedade plena, mas sim reconhece a titularidade e assegura direitos fundamentais relacionados à liberdade, privacidade e intimidade (art. 17).

Art. 17. 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.

O art. 17 da LGPD garante aos titulares os direitos fundamentais de liberdade, intimidade e privacidade. Mais além, no decorrer do Capítulo III (“Dos direitos do titular”), vários outros direitos são assegurados (art.18). Cumpre salientar os direitos de acesso, de notificação, de retificação, de cancelamento e bloqueio dos dados e de não se ficar sujeito a uma decisão individual automatizada, bem como o direito à portabilidade, único que ainda não tinha algum contorno definido antes da LGPD.

Esse modelo normativo não estabelece um domínio absoluto sobre os dados, mas assegura ao titular prerrogativas de controle, como acesso, correção, portabilidade, exclusão e oposição a decisões automatizadas (art. 18), dentro de um regime jurídico finalístico, proporcional e voltado à proteção da dignidade humana.

O tratamento de dados pessoais consiste em qualquer operação realizada com essas informações, conforme definido no art. 5º, inciso X, da Lei Geral de Proteção de

Dados (LGPD). Isso inclui atividades como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração de dados.

No ordenamento jurídico brasileiro, esse tratamento somente é admitido quando amparado por uma das bases legais previstas no art. 7º da LGPD, sendo o consentimento expresso do titular a hipótese mais frequentemente utilizada. Esse consentimento deve ser livre, informado, específico e inequívoco, justamente para garantir que o titular mantenha sua autonomia e não seja reduzido a um mero objeto passivo na cadeia informacional. Nesse contexto, destaca-se o princípio da autodeterminação informativa, que assegura ao indivíduo o poder de decisão sobre o uso de seus dados pessoais, atuando como instrumento essencial para mitigar os riscos inerentes à assimetria de poder entre os titulares e os agentes de tratamento.

Um dos objetivos da LGPD foi fortalecer os poderes do titular, permitindo um controle direto sobre seus dados pessoais e os sujeitos beneficiados pelas suas informações. Assim, se por um lado, os dados coletados geram informações úteis para o mercado, este, por sua vez, está submetido ao consentimento (exceto quando o tratamento se fundamente por outra base legal) e ao atendimento dos direitos dos titulares para que possa usufruir das vantagens concebíveis. Desse modo, há um maior equilíbrio na distribuição dos poderes sobre esses ativos tão relevantes nos tempos atuais

Nesse contexto, ao conferir ao titular o poder de decidir sobre o uso de suas informações, a lei sinaliza para um regime jurídico funcional e proporcional, voltado à proteção da personalidade e não à plena disponibilidade dos dados como se fossem simples mercadorias.

A ideia de tratar os dados pessoais como propriedade do indivíduo tem ganhado espaço no debate jurídico contemporâneo, em especial diante da consolidação de modelos de negócio baseados na exploração econômica de informações pessoais. Embora a privacidade tenha sido historicamente compreendida como um direito fundamental de natureza existencial, não são poucos os autores que sustentam a possibilidade de se conferir aos dados pessoais uma dimensão patrimonial analogamente ao que ocorre com a imagem ou a voz. Nesse contexto,

admite-se que o titular possa, sob certas condições, "vender" ou "alugar" seus dados, sem que isso implique, automaticamente, violação da dignidade humana.

Com o crescimento da economia digital, contudo, a ideia de uma dimensão patrimonial dos dados tem ganhado tração. Muitos autores têm defendido que os dados, embora não alienáveis em sentido pleno, podem ser objeto de cessão onerosa, desde que respeitadas condições específicas. A analogia com o direito de imagem é frequentemente utilizada para sustentar essa posição: tal como a imagem pode ser cedida temporariamente para fins comerciais, os dados poderiam seguir lógica similar sempre dentro de balizas constitucionais.

Nesse sentido, Quintiliano (2022) propõe que os dados sejam tratados como *bens patrimoniais condicionados*, cuja circulação econômica só é legítima quando submetida a limitações materiais e formais. Para o autor, a disposição econômica dos dados deve ocorrer de forma condicionada, específica, temporária e revogável – tal como já ocorre com o direito de imagem.

“A venda de dados não pode significar a venda da própria pessoa”, adverte Quintiliano (2022), ao defender que a exploração econômica dos dados deve preservar a centralidade da dignidade humana e da autodeterminação informativa.

Para o autor, os dados pessoais, cuja circulação econômica só é legítima se forem respeitados os princípios constitucionais, os direitos da personalidade e os limites impostos pela LGPD – notadamente o consentimento específico, informado e inequívoco (art. 7º, I), a transparência, e o direito de revogação do consentimento (art. 8º, §5º). A LGPD, embora não proíba expressamente a venda de dados, impõe restrições substanciais à sua realização, exigindo:

- a) consentimento específico, informado e inequívoco (art. 7º, I),
- b) respeito aos princípios da finalidade, necessidade e transparência (art. 6º),
- c) além da possibilidade de revogação do consentimento a qualquer momento (art. 8º, §5º).

Essas exigências derivam da compreensão de que, em contextos de assimetria ou vulnerabilidade, especialmente os marcados pela precariedade informacional, o

simples consentimento pode não ser suficiente para legitimar práticas de exploração econômica dos dados.

Rodrigo Borges Valadão (2025) adota uma perspectiva pragmática: parte do reconhecimento de que a economia digital contemporânea já monetiza, de fato, dados pessoais, e que diversos modelos de negócio, em especial os adotados por grandes plataformas digitais, baseiam-se na coleta massiva e exploração econômica de dados dos usuários, muitas vezes sem qualquer contraprestação direta. Nesse sentido, o autor critica a ausência de mecanismos reais de negociação por parte do titular, que apenas pode aceitar ou recusar as condições contratuais impostas, o que fragiliza o consentimento e compromete a autodeterminação informacional.

Diante disso, o autor propõe um paradigma jurídico funcional inspirado na cessão onerosa de direitos da personalidade como o direito de imagem que viabilize a monetização dos dados de forma controlada, lícita e transparente. A coexistência de dimensões existenciais e patrimoniais nos dados é compatível com o ordenamento jurídico brasileiro, desde que respeitados:

- a) a transparência adaptativa das informações prestadas pelo controlador;
- b) a manifestação de vontade livre e informada por parte do titular;
- c) a inexistência de abusos decorrentes de assimetrias jurídicas, sociais ou econômicas; e;
- d) a possibilidade de revogação do consentimento a qualquer tempo, nos termos do art. 8º, §5º, da LGPD, com garantia de exclusão dos dados (art. 15, II) ou anonimização (art. 18, IV).

O autor reconhece que, na prática atual, grandes plataformas já monetizam dados pessoais em benefício próprio, impondo suas condições contratuais por meio de contratos de adesão. Isso compromete a liberdade do consentimento e enfraquece o controle informacional do titular, que muitas vezes autoriza a exploração econômica de seus dados sem obter qualquer benefício direto.

Ambos os autores reconhecem que os dados pessoais detêm uma dupla natureza: embora não possam ser plenamente assimilados a bens patrimoniais tradicionais, possuem valor econômico e podem integrar relações jurídicas contratuais, desde que sob um modelo de proteção reforçada. A LGPD, ao não atribuir

propriedade plena sobre os dados, opta por um regime de titularidade funcional, que privilegia a proteção da pessoa sobre a lógica da mercadoria.

No plano normativo, a LGPD oferece um modelo equilibrado. Ainda que não exista, no direito brasileiro, uma norma expressa que autorize a monetização do consentimento, tal prática não encontra vedação jurídica, sendo compatível com os fundamentos do ordenamento vigente. Isso porque o sistema positivo brasileiro se orienta, de um lado, pela proteção da autonomia da vontade consagrada no artigo 421 do Código Civil de 2002 e, de outro, por princípios constitucionais que asseguram a liberdade individual (art. 5º, II), a autodeterminação informativa como expressão da dignidade da pessoa humana (art. 1º, III) e a livre iniciativa (art. 170, caput). Soma-se a isso a Lei n. 13.874/2019, que instituiu a Declaração de Direitos de Liberdade Econômica, reforçando garantias de livre mercado e consagrando a primazia da interpretação jurídica favorável à liberdade econômica nas atividades privadas.

É preciso, contudo, reconhecer que o princípio da autonomia da vontade (CF, art. 5º, II) não opera de forma absoluta, uma vez que é limitada por contextos de vulnerabilidade social ou assimetria informacional, nos quais o consentimento por si só pode não ser suficiente para legitimar a prática. A analogia com o direito de imagem se mostra útil para delinear um modelo normativo: cessão temporária, informada, específica e reversível, elementos que permitem conciliar o valor econômico dos dados com a proteção da personalidade.

Negar a realidade econômica dos dados apenas empurra sua circulação para esferas informais, opacas e potencialmente abusivas. Ao contrário, reconhecer sua monetização sob um regime jurídico proporcional e funcional fortalece a posição do titular e promove um ecossistema digital mais justo.

O principal desafio enfrentado pelo legislador e pela doutrina é desenvolver um modelo normativo que reconheça a relevância econômica dos dados pessoais sem comprometer a dignidade do titular. Para tanto, é essencial que esse modelo tenha como pilares a autodeterminação informativa, a função social da informação, o consentimento qualificado e o controle efetivo do titular sobre suas próprias informações.

Dessa forma, a ideia de tratar a privacidade como propriedade exige cautela. A plena disponibilidade econômica dos dados pessoais não pode se sobrepor à sua natureza essencialmente vinculada à personalidade do indivíduo. Embora a LGPD

não proíba expressamente a comercialização dos dados, ela impõe balizas rigorosas para evitar abusos. Ademais, o tratamento dos dados pessoais para fins econômicos, inclusive a sua eventual comercialização, é juridicamente admissível, desde que realizado com base em fundamentos legais legítimos, em especial o consentimento livre, informado e inequívoco, respeitando os princípios da finalidade, necessidade, proporcionalidade e transparência.

Assim, a regulamentação jurídica deve buscar um ponto de equilíbrio que permita a utilização econômica legítima dos dados pessoais sem desrespeitar os princípios constitucionais que asseguram a liberdade, a privacidade e a autodeterminação informativa. A construção de um modelo de monetização responsável, com proteção reforçada e mecanismos reais de controle pelo titular, representa uma via viável para compatibilizar inovação econômica com os direitos fundamentais no ambiente digital.

3.1.2 Limites e Condições para a Comercialização de Dados Pessoais e Atuação dos Data Brokers

A Lei Geral de Proteção de Dados (LGPD) assegura a titularidade dos dados pessoais, mas não os define como propriedade plena. O titular detém direitos sobre seus dados no contexto de um regime jurídico voltado à proteção da personalidade, o que veda sua mercantilização irrestrita. Assim, a exploração econômica dessas informações deve respeitar os limites éticos, constitucionais e legais, garantindo a observância dos direitos fundamentais e da dignidade da pessoa humana.

O consentimento, embora necessário, não afasta o dever de proteger o titular, especialmente em contextos de vulnerabilidade econômica, social ou informacional. A exploração de dados nesses cenários pode configurar violação à dignidade humana.

Além disso, a intransmissibilidade de certos direitos fundamentais, como o direito à privacidade, é uma proteção constitucional que impede que se "comercializem" certos aspectos da personalidade humana. A LGPD reconhece essas limitações ao estabelecer a necessidade de consentimento informado e ao garantir a segurança e transparência no uso de dados, protegendo o titular contra práticas abusivas de empresas e *data brokers*.

A atuação dos *data brokers*, embora legítima sob a ótica da autonomia contratual e da autodeterminação informativa, está sujeita a uma série de restrições

jurídicas e éticas que visam proteger os direitos fundamentais dos indivíduos. A legislação brasileira, por meio da LGPD (2018) e do Marco Civil da Internet (2014), oferece um quadro jurídico para regular essa comercialização, mas a evolução tecnológica e as práticas de coleta de dados exigem vigilância contínua e adaptação das normas para garantir a proteção efetiva da privacidade no contexto digital.

A atuação dos *data brokers* é emblemática da exploração indireta dos dados pessoais. Essas empresas especializadas atuam como intermediárias, coletando, organizando e revendendo grandes volumes de dados provenientes de diversas fontes, muitas vezes sem o consentimento claro dos titulares.

Esse modelo de negócio coloca em xeque a efetividade da autodeterminação informativa e expõe os indivíduos à hipervulnerabilidade informacional, dado que raramente têm controle ou sequer conhecimento sobre a circulação de suas informações.

Apesar de aspectos legítimos sob a ótica da autonomia informativa, a comercialização de dados exige uma regulação robusta, que proteja os indivíduos contra abusos. A LGPD estabelece diretrizes para tratamento e comercialização, mas a eficácia dessa proteção depende da aplicação ética dos princípios legais como transparência, consentimento explícito e segurança.

A análise dos conceitos de comercialização e monetização de dados pessoais revela a complexidade do cenário contemporâneo de exploração econômica da informação. Ao mesmo tempo em que os dados constituem ativos valiosos para a inovação e o desenvolvimento de novos modelos de negócio, sua manipulação envolve riscos relevantes aos direitos fundamentais.

A legislação brasileira oferece balizas importantes para a proteção do titular, mas seu êxito depende de uma atuação vigilante das autoridades, da sociedade civil e das próprias organizações. Reconhecer os limites jurídicos e éticos à comercialização de dados é essencial para assegurar uma economia digital mais justa, transparente e centrada na pessoa humana.

Por fim, entende-se que diante da sofisticação dos modelos de negócios e do avanço das tecnologias, o ordenamento jurídico deve evoluir para garantir que o uso comercial dos dados pessoais ocorra dentro de parâmetros de proteção da personalidade, da dignidade humana e dos direitos fundamentais.

3.1.3 O Caso da *Tools For Humanity* e a Comercialização de Dados Biométricos

O caso da *Tools For Humanity*, especialmente no contexto de seu projeto *Worldcoin*, insere-se diretamente no debate sobre a comercialização de dados pessoais, particularmente no que diz respeito à coleta e ao uso de dados biométricos. Embora a empresa não se classifique formalmente como um *data broker* tradicional, sua utilização de dados biométricos para criar identidades digitais levanta questões significativas sobre a exploração econômica dessas informações sensíveis. O modelo proposto pelo *Worldcoin*, que oferece um ativo digital em troca do escaneamento da íris dos indivíduos, sugere uma conversão indireta dos dados biométricos em valor monetário. Essa prática coloca em questão as fronteiras da privacidade e da propriedade dos dados, já que indivíduos podem ser incentivados a compartilhar dados altamente pessoais em troca de benefícios financeiros.

Em resposta à crescente preocupação pública, a Autoridade Nacional de Proteção de Dados (ANPD) suspendeu temporariamente a coleta de dados pela *Tools For Humanity*, como parte de um processo de fiscalização (Processo: 00261.006742/2024-53). Esta ação evidenciou os riscos de uma possível utilização indevida de dados biométricos, destacando a necessidade urgente de uma regulamentação mais robusta para proteger os titulares de dados. O modelo de negócios da empresa suscitou importantes questionamentos éticos e jurídicos sobre a autonomia dos indivíduos na gestão de seus dados biométricos, especialmente em regiões com maior vulnerabilidade econômica, onde o consentimento pode ser facilmente manipulado. (Autoridade Nacional de Proteção de Dados, 2025).

O Procon-SP também se manifestou sobre o caso, solicitando esclarecimentos sobre diversos aspectos do projeto, como a forma de apresentação do serviço ao consumidor, o armazenamento e processamento do World ID, as garantias de proteção de dados e os objetivos futuros da iniciativa. Luiz Orsatti Filho, diretor-executivo do Procon-SP, enfatizou a necessidade de uma avaliação rigorosa para assegurar que o projeto atenda aos direitos dos consumidores e esteja em conformidade com o Código de Defesa do Consumidor e outras legislações relevantes, como a Lei Geral de Proteção de Dados (LGPD).

Para Luiz Orsatti Filho, diretor-executivo do Procon-SP, a iniciativa exige uma avaliação rigorosa.

Trata-se de uma tecnologia disruptiva que precisa ser muito bem detalhada, para que possamos verificar se atende ao Código de Defesa do Consumidor e outras legislações, como a que está sendo conduzida pela ANPD.

Entre os pontos levantados, o órgão pediu esclarecimentos sobre:

- Como o serviço é explicado ao consumidor, considerando diferentes níveis de entendimento da população sobre tecnologia;
- Onde e como o World ID é armazenado e processado;
- Quais garantias são oferecidas para a proteção desses dados;
- Os objetivos e usos futuros dessas informações e da remuneração oferecida.
- Outro questionamento relevante é se a proposta da Worldcoin configura um ato de consumo.

A empresa paga usuários pelo escaneamento de sua íris, mas sem um contrato de compra e venda tradicional, o que exige uma análise detalhada para garantir a transparência e direitos dos consumidores, disse Orsatti. (PROCON-SP [...], 2025).

Outro ponto crítico é a caracterização da proposta da Worldcoin como um ato de consumo. A empresa paga aos usuários pelo escaneamento da íris, mas sem um contrato tradicional de compra e venda, o que exige uma análise detalhada para garantir a transparência e a proteção dos direitos dos consumidores.

A Tools for Humanity, por sua vez, afirma que está em conformidade com a LGPD e outras legislações de proteção de dados dos países onde opera. A empresa reforça que adota elevados padrões de privacidade e segurança para proteger as informações coletadas.

A empresa Tools for Humanity (TFH) apresentou à Autoridade Nacional de Proteção de Dados (ANPD) o projeto Worldcoin, que propõe um sistema global de autenticação de identidade baseado no World ID. O sistema utiliza dados biométricos, coletados por meio do dispositivo "Orb", para comprovar que os usuários são humanos reais. A Fundação World em matéria ao Mobile Time declara:

Não é incomum que ideias inovadoras e novas tecnologias levistem questões. A Fundação World acredita que é importante que os reguladores busquem informações ou esclarecimentos sobre suas preocupações. A Fundação World está em total conformidade com todas as leis e regulamentos aplicáveis que regem o processamento de dados pessoais nos mercados onde a World opera. Isso inclui, mas não se limita à Lei de Proteção de Dados Pessoais do Brasil ou LGPD (13.709/2018). Por meio do uso de tecnologia de ponta, a World define os mais altos padrões de privacidade e segurança e incorpora recursos avançados de preservação da privacidade.

A Fundação World dá alta prioridade ao envolvimento com indivíduos e organizações para responder a quaisquer perguntas que possam ter e garantir a transparência em nossas operações e continuará a colaborar ativamente e oferecer as informações necessárias para garantir a compreensão completa de sua tecnologia. (Buctcher, 2025),

No entanto, a proposta da Tools For Humanity tem gerado preocupações tanto no Brasil quanto internacionalmente. O Instituto Brasileiro de Defesa do Consumidor (IDEC) alertou sobre o risco de exploração de grupos socioeconomicamente vulneráveis, que podem não entender plenamente os riscos envolvidos na coleta de seus dados biométricos.

A comercialização desses dados, especialmente em troca de benefícios financeiros, é particularmente problemática, pois pode induzir a exploração de grupos socioeconomicamente mais vulneráveis. A captura de informações biométricas de indivíduos com dificuldades financeiras, que podem não compreender completamente os riscos envolvidos, cria um cenário de potencial abuso. Além disso, a falta de uma regulamentação rigorosa e específica sobre esse tipo de atividade no Brasil abre margem para práticas prejudiciais, que podem comprometer a privacidade e a segurança dos usuários. (CONJUR, 2025),

O tratamento desses dados envolve a captura e processamento de imagens da íris, olhos e rosto, gerando identificadores únicos. Apesar da empresa alegar conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), autoridades internacionais, como a Comissão Nacional de Proteção de Dados de Portugal (CNPD) e a Agência Espanhola de Proteção de Dados (AEPD), já impuseram restrições ao projeto devido a preocupações sobre privacidade e proteção de dados.

Este caso levanta questões importantes sobre a privacidade como uma forma de propriedade e sobre a autodeterminação informativa dos indivíduos. Embora os participantes do projeto Worldcoin possam consentir em trocar seus dados biométricos por criptomoedas, a LGPD impõe limites claros sobre o tratamento de dados sensíveis, exigindo consentimento explícito, além de robustos mecanismos de segurança e transparência. A ANPD considerou que a Tools For Humanity não atendeu adequadamente a esses requisitos, o que levou à suspensão temporária de suas atividades de coleta de dados no Brasil.

Portanto, o caso da Tools For Humanity ilustra a complexidade e os desafios da comercialização de dados pessoais, especialmente dados biométricos. Embora a empresa não se enquadre diretamente como um *data broker* tradicional, seu modelo de negócios revela as nuances e os riscos associados à exploração comercial de dados sensíveis. Este episódio destaca a necessidade urgente de um debate profundo sobre até que ponto a comercialização de dados pessoais pode ser realizada de maneira legal e ética, sem comprometer os direitos fundamentais dos indivíduos à

privacidade e à proteção de seus dados pessoais. Para que a comercialização de dados seja permitida, é imprescindível que os direitos de privacidade e a proteção dos dados pessoais sejam respeitados de forma transparente e responsável.

Em última análise, a experiência da TFH ilustra com nitidez o conflito entre o valor econômico dos dados pessoais e sua natureza existencial. A solução normativa e ética para esse dilema não pode se apoiar exclusivamente na lógica contratual ou na autonomia da vontade, mas deve estar ancorada nos princípios da dignidade humana, da função social da informação e do consentimento qualificado e informado.

3.2 Coleta e Processamento de Dados

A comercialização de dados pessoais tornou-se um dos pilares fundamentais da economia digital moderna, com os *data brokers* desempenhando um papel central na coleta, processamento e análise de informações pessoais. Este fenômeno, embora tenha gerado imensas oportunidades comerciais, também levanta questões críticas sobre privacidade, ética e a proteção dos direitos dos indivíduos.

A coleta de dados é a base do funcionamento dos *data brokers*. Estes agentes especializados utilizam diversas fontes e métodos tecnológicos para reunir informações pessoais e comportamentais. As principais fontes de dados incluem:

- a) **Redes sociais:** Informações publicadas pelos usuários em plataformas como Facebook (Meta), Instagram, Twitter e LinkedIn;
- b) **Registros públicos:** Dados disponíveis em fontes governamentais, como registros de propriedade e informações judiciais;
- c) **Transações comerciais:** Registros de compras, interações de clientes com plataformas de e-commerce e históricos financeiros;
- d) **Plataformas digitais:** Interações com sites e aplicativos, como pesquisas de navegação e comportamento online.

Importante destacar que os corretores de dados não obtêm essas informações diretamente dos consumidores, o que significa que a grande maioria das pessoas não tem consciência de que seus dados estão sendo coletados e utilizados dessa forma. Embora cada fonte de dados forneça apenas uma pequena parte do perfil de um consumidor, os corretores de dados são capazes de combinar essas informações fragmentadas para criar um retrato muito mais detalhado da vida do indivíduo.

Os *data brokers* empregam técnicas automatizadas como *web scraping*, *APIs* e a compra de dados de terceiros para reunir um volume massivo de informações, muitas vezes sem o conhecimento ou controle dos indivíduos sobre o processo.

Após a coleta, os dados passam por processos de agregação e análise para criar perfis detalhados dos indivíduos. Essas etapas envolvem a segmentação dos dados com base em características demográficas (como idade, gênero e localização), comportamentais (hábitos de consumo) e psicográficas (valores e preferências). O objetivo é compreender as necessidades e preferências do consumidor de forma a permitir a personalização de ofertas e campanhas publicitárias.

Os *data brokers* desempenham um papel fundamental neste processo, agregando dados de diversas fontes e utilizando análises preditivas para inferir comportamentos futuros. Isso permite a segmentação eficaz de mercados, a melhoria da experiência do cliente e a criação de modelos de negócios baseados em dados.

No entanto, essa prática de segmentação e análise de dados levanta preocupações em relação à privacidade e ao consentimento dos indivíduos, especialmente quando as informações são utilizadas sem o devido conhecimento ou autorização dos consumidores. A crescente complexidade do uso de dados pessoais em diferentes contextos exige uma atenção especial às implicações éticas e legais desse processo.

A coleta massiva de informações pessoais pelos *data brokers* teve um impacto profundo no comportamento do mercado. A personalização de ofertas e a segmentação de consumidores tornaram-se práticas comuns, permitindo que as empresas direcionem suas campanhas de marketing de forma mais eficaz.

A evolução dessa indústria reflete as mudanças nas práticas comerciais e as demandas por dados na era digital. No entanto, as preocupações em torno da privacidade e da ética no uso de dados pessoais exigem uma análise crítica e um entendimento profundo das implicações legais e sociais desse fenômeno.

3.3 Aplicações Comerciais dos Dados Pessoais: Setores e Modelos de Negócios

O mercado de dados pessoais se consolidou como uma dinâmica comercial crescente, com diversas empresas de setores variados utilizando esses dados para impulsionar estratégias de marketing, finanças, entre outros segmentos. Nesse cenário, os *data brokers* (corretores de dados) desempenham um papel central,

atuando como intermediários que coletam, analisam e comercializam dados pessoais de consumidores para uma ampla gama de indústrias, incluindo publicidade, finanças e saúde.

Empresas como Meta, Google e Amazon, além de instituições financeiras e outras grandes corporações, lideram essa economia digital ao desenvolver modelos de negócios baseados na exploração de dados pessoais. Essas organizações utilizam dados para personalizar ofertas, otimizar campanhas publicitárias e criar produtos e serviços que atendem de forma mais eficiente às necessidades dos consumidores.

A Experian (conhecida no Brasil como Serasa Experian), Epsilon e CoreLogic se consolidaram como líderes nesse setor, sendo a corretora de dados financeiros.

Sampaio (2017) exemplifica três empresas que exploram os rastros informacionais dos indivíduos: Acxiom Corp (*data broker*), Google (internet) e a NSA (agência governamental dos EUA). A Acxiom Corp, uma das maiores corretoras de dados do mundo, coleta interações online e offline. O Google se destaca pela captação e processamento massivo de dados, enquanto a NSA mantém uma relação estreita com o Google para compartilhamento de informações. De acordo com Sampaio (2017), "essas entidades transformam dados em capital através de transações comerciais e políticas", revendendo dados minerados para diversas indústrias, como financiadoras, bancos e farmacêuticas.

[...] São empresas baseadas na obtenção de lucros através da extração de dados pessoais coletados por meio de interações de atividades humanas tecnicamente mediadas por máquinas criando uma rede ilimitada de conhecimento. Esse tipo de vigilância corporativa, de capacidade aparentemente infinita, atua especialmente na coleta e tratamento de dados para construção de categorizações que funcionam como um modelo de predição do futuro. (Sampaio, 2017, p. 31).

Esse mercado é caracterizado pela troca de informações pessoais e comportamentais, frequentemente intermediada pelos *data brokers*. Entretanto, essa dinâmica também apresenta riscos legais, como a responsabilidade por vazamentos ou uso inadequado de dados.

Essas informações captadas, monitoradas e exploradas podem ser utilizadas de forma inadequada ou até invasiva, interferindo, por exemplo, em contratos de seguro de vida, empréstimos, contratação de trabalho, planos de saúde, além do uso para o marketing direcionado. (Sampaio, 2017, p.19).

A regulamentação de dados, como a Lei Geral de Proteção de Dados nº 13.709/18 (LGPD) no Brasil, o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia e legislações comparadas, surgiram para mitigar esses riscos, promovendo maior transparência e proteção no tratamento de dados pessoais.

3.3.1 Interseção entre Direito e economia

No contexto dessa economia digital, a interseção entre Direito e economia é clara. Richard Posner, em sua obra *Economic Analysis of Law* (2007), descreve o mercado como um sistema dinâmico onde compradores e vendedores interagem, moldados por fatores legais que influenciam as condições de troca. O Direito, segundo Posner, facilita transações ao garantir previsibilidade e segurança jurídica, elementos essenciais no mercado de dados pessoais.

Posner (2007) apresenta uma análise abrangente do conceito de mercado, enfatizando a interseção entre economia e Direito. Para o autor, um mercado não é meramente um local físico ou virtual, mas um sistema dinâmico de troca onde compradores e vendedores interagem continuamente. Essas interações são fundamentais para a determinação do preço e da quantidade de bens e serviços disponíveis, sendo influenciadas por fatores legais e institucionais que moldam as condições de mercado.

O autor define o mercado como um espaço onde a oferta e a demanda se encontram, destacando que o preço é determinado por essas forças. Ele argumenta que o Direito desempenha um papel essencial na facilitação das transações de mercado, assegurando que as relações comerciais ocorram de maneira eficiente e justa. As regras legais que regem contratos, propriedade e responsabilidade são vistas como pilares fundamentais para o funcionamento eficaz do mercado, uma vez que garantem a previsibilidade e a segurança jurídica necessária para a confiança dos agentes econômicos.

Segundo Ronald Coase (COASE, 1937), *"A empresa consiste no sistema de relações que ganham vida quando a direção de recursos é dependente do empreendedor."* Esses custos de transação envolvem não apenas o custo monetário de cada fator de produção, mas também o tempo e os recursos gastos na negociação, elaboração e cumprimento dos contratos que garantem o funcionamento das transações empresariais.

A partir dessa perspectiva, podemos refletir sobre vários aspectos importantes:

a) Contratos e Troca de Dados

No emergente mercado de dados, empresas e *data brokers* atuam como intermediários em transações que envolvem a troca de dados pessoais e comportamentais. As regras contratuais que regulam essas transações são cruciais, pois garantem que as partes envolvidas cumpram suas obrigações. Por exemplo, um contrato de licenciamento de dados pode estabelecer limites claros sobre como as informações podem ser utilizadas, protegendo tanto os direitos dos consumidores quanto os interesses das empresas.

b) Regulação de Dados Pessoais

A atuação dos *data brokers* é fortemente influenciada por normas jurídicas internacionais, e pela Lei Geral de Proteção de Dados (LGPD) no Brasil. Essa legislação estabelece requisitos rigorosos sobre a coleta, o armazenamento e a comercialização de dados pessoais, impactando diretamente a operação desses intermediários. A conformidade esperada com a LGPD não apenas garante a proteção dos direitos dos titulares de dados, mas também pode moldar as práticas comerciais e estratégias dos *data brokers*.

c) Responsabilidade e Risco

A responsabilidade legal tem um papel significativo nas decisões econômicas. No contexto do mercado de dados, a ocorrência de vazamentos de dados ou o uso indevido de informações pessoais podem desencadear ações judiciais significativas. A possibilidade de litígios e sanções legais leva os *data brokers* a adotar práticas mais rigorosas de gestão de dados, e consentimento de usos, minimizando riscos e protegendo sua reputação no mercado.

d) Concorrência e Inovação

A concorrência entre *data brokers* pode servir como um motor para a inovação em métodos de coleta, processamento e análise de dados. Nesse contexto, as normas de propriedade intelectual e as regras contra práticas comerciais desleais desempenham um papel central na definição da dinâmica competitiva. Por exemplo,

um *data broker* que desenvolve uma tecnologia inovadora para análise de dados pode conquistar uma vantagem competitiva significativa, aprimorando a eficiência e diversificando as opções disponíveis para consumidores e empresas que buscam insights baseados em dados.

A interação entre normas jurídicas e dinâmicas de mercado é essencial para garantir eficiência e equidade, e o mercado de dados pessoais é um exemplo claro disso. As leis não apenas regulam as interações entre agentes econômicos, mas também asseguram que o mercado opere de forma justa e produtiva.

O avanço da digitalização e a crescente importância da proteção de dados tornam crucial uma abordagem integrada entre os aspectos econômicos e legais nas transações de dados. Nesse cenário, a sinergia entre Direito e Economia não é apenas desejável, mas essencial para moldar um mercado mais equilibrado e inovador.

3.4 A Valorização dos Dados Pessoais no Mercado Global: Aplicação do Setor empresarial

O setor empresarial é um dos maiores beneficiários da indústria de dados, com os *data brokers* oferecendo serviços que permitem às empresas desenvolver estratégias de marketing mais eficazes, prever o comportamento do consumidor e avaliar riscos em operações financeiras. Esses agentes desempenham um papel estratégico ao fornecer insights detalhados, que são utilizados para personalizar produtos e serviços, elevando a competitividade das empresas.

As principais aplicações dessa comercialização de dados no ambiente empresarial incluem:

- a) **Marketing direcionado:** As empresas utilizam os dados coletados pelos *data brokers* para realizar campanhas publicitárias altamente segmentadas. Ao acessar informações detalhadas sobre comportamentos de consumo, localização geográfica, preferências pessoais e até características psicográficas dos indivíduos, as marcas podem otimizar seus anúncios, tornando-os mais relevantes e personalizados. Isso aumenta a eficácia das campanhas e o retorno sobre investimento (ROI), ao atingir diretamente consumidores com maior potencial de conversão.

- b) **Análise de Risco e Crédito:** O setor financeiro se beneficia das capacidades analíticas dos *data brokers* para avaliar a saúde financeira e o risco de crédito dos consumidores. Através da análise de históricos de compras, dados de redes sociais e transações bancárias, as instituições financeiras conseguem uma visão detalhada da situação econômica dos indivíduos. Isso permite a oferta de produtos financeiros mais adequados ao perfil de cada consumidor. No entanto, o uso de dados para análise de crédito levanta questões sobre a opacidade dos algoritmos e o risco de discriminação, uma vez que decisões baseadas em dados podem não ser totalmente transparentes e prejudicar grupos vulneráveis.
- c) **Desenvolvimento de Produtos e Serviços:** Dados pessoais são usados para desenvolver novos produtos e serviços que atendem de forma mais precisa às necessidades e expectativas dos consumidores. A coleta de informações sobre preferências e comportamentos de compra possibilita que as empresas ajustem suas ofertas, criando soluções mais atraentes para o público-alvo. Setores como tecnologia, moda, saúde e entretenimento se beneficiam enormemente desse modelo, criando experiências personalizadas para seus clientes.

3.4.1 Riscos e Benefícios da Comercialização de Dados

Apesar dos benefícios econômicos da comercialização de dados se realizados de forma legítima, essa prática também impõe riscos significativos tanto para as empresas quanto para os consumidores. Para as empresas, o uso excessivo de dados pode gerar dependência, resultando em decisões comerciais baseadas em informações imprecisas ou incompletas. Além disso, o vazamento de dados ou o uso inadequado das informações pode afetar seriamente a reputação da empresa, além de acarretar multas e ações legais, especialmente à luz de regulamentações como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia.

Por outro lado, os consumidores enfrentam riscos diretamente relacionados à privacidade e autonomia. A ausência de controle sobre como seus dados são coletados, processados e compartilhados compromete a segurança de suas informações pessoais, podendo levar a abusos como discriminação, exclusão de

serviços ou ofertas inadequadas. Mais grave ainda é a criação de um ambiente de vigilância constante, onde empresas monitoram comportamentos e preferências sem o conhecimento ou consentimento dos consumidores. Esse cenário pode se estender além do marketing segmentado, com dados pessoais sendo utilizados para restringir o acesso a serviços financeiros, seguros ou até oportunidades de emprego, aprofundando desigualdades sociais e econômicas.

Como destaca Ana Frazão (2020), a ascensão da economia digital acentua preocupações sobre a centralização do poder nas mãos de poucos grandes players, que exploram dados sem supervisão adequada. A falta de transparência nas práticas dos *data brokers* e a ausência de um controle efetivo sobre o uso das informações tornam esse modelo de negócios problemático. A manipulação de dados pessoais sem o consentimento explícito dos consumidores reforça esses problemas, criando um ambiente de grande vulnerabilidade.

A implementação da LGPD no Brasil visa corrigir esse desequilíbrio, criando um ambiente mais seguro e equilibrado para o uso de dados pessoais. Essa legislação estabelece novos paradigmas de regulamentação, que buscam mitigar riscos e garantir os direitos dos consumidores. No entanto, a adaptação dos *data brokers* a essas exigências ainda enfrenta obstáculos significativos, dificultando a proteção plena da privacidade e dos direitos dos indivíduos.

3.4.2 Reflexões sobre os Riscos da Comercialização de Dados Pessoais

A falta de transparência nas práticas de coleta e análise de dados amplia a assimetria de poder entre consumidores e corporações. Impactos Econômicos e Riscos para os Consumidores. Embora os *data brokers* desempenhem um papel estratégico na economia digital, os riscos associados à sua atuação são significativos:

- a) **Falta de Transparência:** Consumidores não têm acesso claro às informações coletadas sobre eles, nem às opções para gerenciar ou excluir esses dados.
- b) **Violações de Privacidade:** A coleta massiva de dados ocorre frequentemente sem consentimento, contrariando princípios fundamentais de proteção de dados.

- c) **Manipulação Comportamental:** Modelos preditivos baseados em dados podem influenciar decisões de consumo, crédito e até oportunidades de emprego, reforçando desigualdades sociais.
- d) **Insegurança de Dados:** O armazenamento de grandes volumes de informações aumenta a exposição a vazamentos e ataques cibernéticos.

Embora regulamentações como a LGPD e o GDPR busquem reverter esse desequilíbrio, sua implementação ainda enfrenta desafios, principalmente devido à falta de adaptação dos *Data brokers* e à complexidade de fiscalização.

Essas leis visam garantir que os dados sejam tratados de forma ética, com consentimento explícito dos consumidores e responsabilidade por parte das empresas. Para que a proteção da privacidade seja eficaz, é essencial que os *data brokers* adotem práticas que promovam a transparência e o respeito aos direitos dos indivíduos.

A implementação de legislações como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia busca enfrentar esses desafios, introduzindo requisitos como:

- a) **Finalidade Específica:** Os dados só podem ser tratados para objetivos legítimos e previamente definidos.
- b) **Consentimento Informado:** A coleta e uso de dados pessoais exigem autorização explícita dos titulares.
- c) **Transparência e Accountability:** Empresas devem adotar práticas claras e sujeitas à fiscalização.

Entretanto, como argumentam Doneda (2019) e Frazão (2020), a simples existência de normas não garante sua eficácia. A fiscalização insuficiente e a rápida evolução tecnológica tornam difícil a aplicação prática desses princípios. Além disso, muitos *data brokers* continuam a operar em descompasso com esses regulamentos, ignorando, por exemplo, o requisito de consentimento livre e informado.

A regulamentação de dados, como o GDPR (2016) e a LGPD (2018), busca reverter esse desequilíbrio, impondo requisitos de transparência, consentimento e responsabilidade aos responsáveis pelo tratamento dos dados. No entanto, como

destaca Ana Frazão (2020), a implementação efetiva dessas leis exige uma fiscalização rigorosa e a adaptação dos modelos de negócio dos *data brokers*, que, em muitos casos, ainda operam à margem da legislação vigente.

Essas regulamentações visam garantir que a coleta e comercialização de dados sejam realizadas de forma ética e transparente, respeitando os direitos fundamentais dos consumidores. Para garantir uma proteção eficaz à privacidade dos indivíduos, é necessário que os *data brokers* adotem práticas que incluam o consentimento explícito dos consumidores, a transparência no uso de dados e a responsabilidade nas operações.

O mercado de dados é altamente lucrativo, e os *data brokers* operam com um modelo de negócios baseado na coleta, processamento e venda de dados. Este modelo oferece às empresas uma vantagem competitiva ao fornecer insights valiosos sobre o comportamento de seus clientes e as tendências de mercado. Setores como marketing, saúde, finanças e tecnologia se beneficiam amplamente dessa economia de dados. No entanto, a concentração de poder nas mãos de poucos players dominantes, como Google e Facebook (Meta), e a falta de transparência nas práticas de coleta de dados sem consentimento explícito, geram uma necessidade urgente de regulamentação eficaz.

Embora leis como a LGPD e o GDPR tenham sido passos importantes na direção de maior controle sobre o uso de dados pessoais, a adaptação dos *data brokers* a essas regulamentações continua sendo um desafio. Para garantir uma proteção robusta da privacidade, é fundamental que as empresas adaptem suas práticas de coleta e uso de dados, priorizando os direitos dos consumidores.

3.4.4 Desafios e Necessidade de uma Regulação Eficaz

A comercialização de dados pessoais constitui um desafio significativo para reguladores, acadêmicos e advogados, exigindo uma análise cuidadosa e uma adaptação constante às novas demandas do mercado. De acordo com Ana Frazão, é urgente repensar o modelo de negócios dos *data brokers*, especialmente à luz de legislações emergentes de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia. Esses marcos legais destacam a necessidade de maior transparência, consentimento informado e responsabilidade no uso dos dados

peçoais, aspectos ainda a serem totalmente incorporados pelos intermediários do mercado de dados, com o objetivo de garantir a privacidade dos consumidores.

Embora o modelo de negócios dos *data brokers* impulse a inovação e a personalização no mercado, ele também impõe desafios éticos e legais significativos. A regulamentação rigorosa é essencial para assegurar que os dados pessoais sejam tratados de maneira ética e transparente, respeitando os direitos dos indivíduos. O equilíbrio entre inovação tecnológica e a proteção dos direitos dos consumidores será crucial para o desenvolvimento sustentável e justo da economia digital.

Na economia digital atual, os dados pessoais adquiriram um valor considerável, sendo essenciais para a criação de perfis detalhados dos consumidores. As empresas se beneficiam dessa coleta de dados para segmentar suas ofertas de forma mais precisa, promovendo serviços personalizados, campanhas de marketing direcionadas e otimização de ofertas financeiras. O papel dos *data brokers*, portanto, é fundamental nesse processo, uma vez que eles agregam informações de diversas fontes – comportamentos online, interações em plataformas digitais, transações financeiras, entre outros – para construir perfis sofisticados dos indivíduos.

No entanto, o uso desses dados, especialmente sem o conhecimento explícito dos consumidores, levanta questões cruciais sobre privacidade e consentimento. Ao contrário dos mercados tradicionais, em que as transações são mais transparentes, o mercado de dados opera frequentemente em um ambiente de opacidade. Os consumidores muitas vezes não sabem como suas informações estão sendo utilizadas ou compartilhadas, o que cria um cenário de vulnerabilidade e desconfiança. Esse problema se intensifica com a falta de uma regulação eficaz que exija transparência sobre as práticas de coleta e comercialização de dados.

À medida que as interações digitais se tornam mais integradas ao cotidiano, organizações de diversos setores – de redes sociais a plataformas de e-commerce – coletam dados pessoais com o intuito de elaborar perfis detalhados e personalizados sobre os indivíduos. Esses dados, frequentemente compartilhados com outros agentes do mercado, alimentam a cadeia de comercialização de informações, envolvendo desde grandes empresas de tecnologia como Facebook (Meta) e Google até corretoras de dados, conhecidas como *data brokers*. Estes intermediários desempenham um papel central na circulação de dados, influenciando como as

empresas se comunicam com os consumidores e como os produtos e serviços são oferecidos.

Além das gigantes tecnológicas, outras entidades, como birôs de crédito e empresas especializadas em informações financeiras, também estão profundamente envolvidas no processo de segmentação de mercado. Elas recolhem e processam dados financeiros, como históricos de pagamento e pontuações de crédito, sendo essenciais na avaliação de riscos financeiros e no ajuste de ofertas de crédito. Este uso de dados pessoais para fins de classificação e score de crédito revela o impacto considerável que esses intermediários podem ter sobre as oportunidades econômicas dos indivíduos, sublinhando a necessidade de uma regulamentação robusta que proteja os direitos dos consumidores nesse novo mercado.

3.5 A Fragmentação e o Mercado Global de Dados: O Papel das Empresas Multinacionais

A fragmentação do mercado de dados pessoais e o papel das empresas multinacionais tornam o cenário global ainda mais complexo. Grandes corporações como Meta (Facebook), Google, Amazon e instituições financeiras dominam o mercado, coletando dados de diversas fontes e criando perfis detalhados dos consumidores. Além disso, entidades como birôs de crédito e empresas especializadas em informações financeiras desempenham um papel crucial no processo de segmentação e definição de riscos financeiros, exercendo um controle na comercialização de dados pessoais.

O relatório da *Federal Trade Commission (FTC) de 2014, Data brokers: A Call for Transparency and Accountability*, destaca como a atuação dos *Data brokers* impacta a economia digital, com muitos consumidores desconhecendo a diversidade de práticas adotadas por esses intermediários. A falta de transparência nas práticas de coleta e uso de dados pessoais cria um ambiente onde os consumidores perdem o controle sobre suas próprias informações.

Os dados obtidos abrangem uma ampla gama, incluindo registros comerciais, informações governamentais e conteúdos de redes sociais e blogs. Essa complexidade aumenta com a utilização de dados brutos e derivados, que permitem a construção de perfis detalhados a partir de inferências sobre comportamentos e características dos consumidores.

Entre as principais observações do relatório, destaca-se que muitos consumidores desconhecem a existência e a variedade das práticas dos *data brokers*. A coleta de dados muitas vezes ocorre sem o conhecimento ou consentimento explícito dos indivíduos, criando um ambiente opaco que dificulta a transparência necessária. Além disso, a combinação de dados *online* e *offline* para direcionar consumidores em ambientes digitais revela a sofisticação das operações dessa indústria.

Embora a atuação dos *data brokers* possa trazer benefícios, como a melhoria de serviços de marketing e a mitigação de riscos, os perigos associados à coleta e ao uso inadequado dos dados são significativos. A falta de transparência nas escolhas oferecidas aos consumidores e a complexidade do sistema de dados apresentam desafios regulatórios substanciais.

Esses intermediários, muitas vezes, coletam dados sem o consentimento explícito dos consumidores, criando uma situação de assimetria informacional que dificulta a regulação e a proteção de dados. O aumento da digitalização e a globalização desse mercado exigem uma abordagem regulatória eficaz, que garanta tanto a proteção dos direitos dos indivíduos quanto a inovação no uso de dados pessoais.

Além disso, a fragmentação do mercado de dados, com a atuação de múltiplos agentes em diversas regiões, aumenta os desafios para a implementação de regulamentações globais. Empresas multinacionais frequentemente enfrentam dificuldades para aderir às regulamentações locais, como a LGPD no Brasil ou o GDPR na União Europeia, o que ressalta a necessidade urgente de uma regulamentação mais eficiente e harmonizada a nível global.

Diante desse cenário, é crucial que sejam implementadas ações eficazes para garantir que os *data brokers* se ajustem às exigências legais emergentes, minimizando os efeitos prejudiciais de suas operações até então não regulamentadas. A proteção dos dados pessoais deve ser uma prioridade, refletindo a responsabilidade ética dos agentes envolvidos na coleta e no tratamento de informações sensíveis. A evolução contínua nesse campo requer vigilância constante e uma abordagem proativa na regulamentação do mercado de dados pessoais.

4 ASPECTOS LEGAIS E DESAFIOS REGULATÓRIOS

4.1 A Evolução das Normativas de Proteção de Dados

Com a aceleração da digitalização e a crescente interconectividade global, a proteção dos consumidores e a conformidade legal emergem como prioridades essenciais em diversas regiões do mundo, incluindo a União Europeia e o Brasil. Este capítulo examina as principais normativas internacionais que regem a comercialização de dados pessoais, com especial foco na Lei Geral de Proteção de Dados (LGPD) do Brasil, no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e na Lei de Privacidade do Consumidor da Califórnia (CCPA). A análise aborda os impactos dessas legislações sobre as práticas de comercialização de dados realizadas pelos *data brokers*.

4.1.1. Regulamentação no Brasil

A sociedade contemporânea tem vivido uma transformação social, econômica e cultural impulsionada pela tecnologia, que desempenha um papel central nesse processo. Com a globalização e o surgimento de inovações tecnológicas como a Internet das Coisas, aprendizado de máquina e inteligência artificial, o interesse por dados tem crescido de maneira exponencial. Hoje, os dados são frequentemente descritos como o "novo petróleo", devido ao seu valor estratégico no mercado global.

A popularização da internet e o advento das redes sociais mudaram profundamente as formas de relacionamento e socialização de informações. A simples ação de "curtir" uma postagem no Facebook ou Instagram, por exemplo, reflete as preferências e interesses pessoais de um indivíduo. Nos últimos anos, práticas de coleta de informações pessoais se tornaram mais sofisticadas. Com o aumento do compartilhamento de dados em transações cotidianas, como a compra de um livro online, surgiram preocupações sobre a privacidade, exigindo regulamentação e a criação de normas e regras para o uso e tratamento de dados pelas empresas.

Em 2012, a União Europeia deu um passo importante ao estabelecer um marco regulatório para a proteção da privacidade online, com a criação do Regulamento Geral sobre a Proteção de Dados (GDPR), aprovado em 2016. O GDPR é amplamente reconhecido como o mais robusto conjunto de medidas de proteção de

dados pessoais desde a criação da internet, forçando empresas globais, como Facebook e Google, a revisar suas práticas de coleta e uso de dados. Esse regulamento inspirou diversos países a implementarem legislações semelhantes, como a Lei de Privacidade do Consumidor da Califórnia (CCPA) nos Estados Unidos e a Lei Geral de Proteção de Dados (LGPD) no Brasil, instituída pela Lei nº 13.709 de 2018.

A promulgação da LGPD trouxe uma nova visão sobre a privacidade digital no Brasil. Embora o conceito de privacidade seja frequentemente associado à vida íntima ou pessoal, o seu significado vai além disso. O direito à privacidade remonta à Antiguidade, onde estava ligado à proteção da vida cotidiana e do sentimento pessoal, sendo um privilégio de classes mais abastadas. No contexto atual, no entanto, a privacidade não se limita apenas ao isolamento, mas à proteção dos dados pessoais, que têm grande valor no cenário digital.

No Brasil, o direito à privacidade é garantido pela Constituição de 1988, em seu Artigo 5º, inciso X, que assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como o direito à proteção de dados. Além disso, o Código Civil, em seu Artigo 21, reforça a proteção à vida privada, permitindo que o juiz adote medidas para impedir a violação desses direitos.

Com a popularização de redes sociais como Facebook (Meta), Twitter e Instagram, além de gigantes do comércio eletrônico como Amazon, a interação entre pessoas e empresas passou a ser mediada pela internet, o que modificou a forma como nos relacionamos e compartilhamos informações. Esse novo ambiente gerou uma nova "matéria-prima": os dados pessoais. Esses dados passaram a ser explorados a partir da criação do Marco Civil da Internet (Lei nº 12.965/2014), que regula os direitos e deveres dos usuários na internet, além de proteger a privacidade e os dados pessoais dos cidadãos brasileiros.

Embora a privacidade digital seja um conceito frequentemente utilizado, é importante distinguir entre privacidade e proteção de dados. Se uma pessoa publica um dado em sua rede social, esse dado se torna público, mas isso não significa que ele pode ser utilizado sem restrições. O uso desses dados deve respeitar os direitos do titular, conforme estabelecido pela LGPD. Dessa forma, os dados estão protegidos pelo princípio da proteção de dados, não pela privacidade constitucional.

A LGPD foi concebida para ampliar e modificar os conceitos presentes no Código Civil de 2002 e no Marco Civil da Internet de 2014. O foco da LGPD é garantir que o tratamento dos dados pessoais seja feito de maneira transparente, segura e responsável, atendendo aos princípios fundamentais da proteção de dados pessoais.

Os dados pessoais são definidos como qualquer informação que possa identificar uma pessoa, seja de forma identificada ou identificável. Além disso, a LGPD traz a definição de dados sensíveis, conforme o Artigo 5º da lei. A legislação também define o que caracteriza o tratamento de dados, englobando todas as operações realizadas com esses dados, como coleta, transmissão, compartilhamento, entre outras.

a) Princípios Fundamentais da Proteção de Dados Pessoais

O Artigo 6º da LGPD estabelece os princípios fundamentais para a proteção dos dados pessoais. Antes de detalhá-los, é importante destacar que a boa-fé no tratamento dos dados pessoais é uma premissa básica. Ou seja, antes de utilizar os dados de um indivíduo, as empresas devem se perguntar: "Qual é a finalidade desse tratamento?" "Esses dados são realmente necessários?" "O consentimento foi dado de forma clara e inequívoca?" "Há risco de discriminação por meio desses dados?"

➤ Os princípios fundamentais estabelecidos pela LGPD são:

- **Finalidade:** o tratamento deve ter uma finalidade específica, informada de forma clara e explícita ao titular dos dados.
- **Adequação:** o tratamento deve ser compatível com a finalidade informada.
- **Necessidade:** a coleta de dados deve ser limitada ao estritamente necessário para cumprir a finalidade.
- **Livre acesso:** o titular deve ter acesso fácil e gratuito às informações sobre como seus dados são tratados.
- **Qualidade dos dados:** os dados devem ser exatos e atualizados conforme a necessidade do tratamento.
- **Transparência:** o titular deve ser informado de forma clara e acessível sobre o tratamento e os responsáveis por ele.
- **Segurança:** as medidas de segurança devem ser implementadas para proteger os dados contra acessos não autorizados, perdas ou danos.

- **Prevenção:** devem ser adotadas medidas para evitar danos ao titular e aos envolvidos no tratamento.
- **Não discriminação:** os dados não podem ser usados para fins discriminatórios ou abusivos.
- **Responsabilização:** as organizações devem ser capazes de demonstrar a eficácia das medidas adotadas para proteger os dados.

b) Direitos dos Titulares e Dados Pessoais

A LGPD garante aos indivíduos o controle sobre seus dados pessoais, empoderando-os em relação à coleta, uso e tratamento dessas informações. O principal objetivo da lei é proteger a liberdade e a privacidade dos cidadãos, assegurando-lhes a titularidade de seus dados pessoais. A partir disso, conforme art. 18, os titulares têm o direito de acessar seus dados, corrigir informações desatualizadas ou incorretas, e até mesmo pedir a eliminação dos dados, caso não sejam mais necessários ou estejam sendo tratados de maneira indevida.

A LGPD estabelece uma série de direitos para os titulares dos dados, como:

- **Confirmação da existência de tratamento:** o direito de saber se seus dados estão sendo tratados.
- **Acesso:** o direito de acessar os dados que uma organização possui sobre o titular.
- **Correção de dados** incompletos ou desatualizados.
- **Anonimização ou eliminação de dados desnecessários:** caso os dados sejam excessivos ou tratados em desacordo com a LGPD.
- **Portabilidade:** o direito de transferir seus dados para outro fornecedor de serviços.
- **Eliminação de dados:** o titular pode solicitar a eliminação dos dados quando retirar o consentimento.
- **Informações sobre compartilhamento de dados:** o direito de saber com quem seus dados foram compartilhados.
- **Revogação do consentimento:** o titular pode revogar o consentimento dado previamente para o tratamento de seus dados.

Com a LGPD, o Brasil deu um importante passo na proteção da privacidade e dos dados pessoais de seus cidadãos, alinhando-se a uma tendência global de maior controle sobre as informações digitais.

4.1.2 GDPR (*General Data Protection Regulation*)

Na década de 1960, o filósofo e educador canadense *Marshall McLuhan* (1911-1980), um dos pioneiros nos estudos sobre a comunicação e seu impacto na sociedade, antecipava a popularização de tecnologias como a internet e a emergência de um mundo digital interconectado. *McLuhan* defendia que os meios de comunicação funcionavam como extensões do ser humano, proporcionando novas formas de percepção e interação com o mundo à sua volta (Costa, 2011).

Essas previsões começaram a se concretizar com o lançamento do primeiro computador em 1977, e, com o tempo, a evolução tecnológica levou ao surgimento de inovações como a internet, os telefones celulares e as redes sociais. Esses avanços estabeleceram novas formas de relacionamento e socialização, tornando difícil imaginar a vida moderna sem dispositivos móveis e acesso contínuo à rede.

Em um mundo hiperconectado, onde o tráfego de dados pessoais é cada vez mais intenso, surgiram questões éticas e desafios relacionados ao uso e ao controle desses dados, criando a necessidade urgente de ferramentas regulatórias que pudessem controlar o uso indiscriminado das informações pessoais no ambiente digital.

Com a crescente utilização de dados pessoais por empresas e entidades públicas e privadas, vários países adotaram legislações para regulamentar o uso desses dados. Entre as iniciativas pioneiras está o Regulamento Geral sobre a Proteção de Dados (GDPR, na sigla em inglês), aplicável aos países da União Europeia e às empresas que tratam dados de cidadãos da região. Antes da implementação do GDPR, a União Europeia já possuía leis de privacidade (como a Diretiva 95/46/CE de 1995), mas estas não eram adequadas ao contexto tecnológico atual.

O projeto do GDPR teve início em 2012 e foi aprovado em 2016, sendo que sua implementação gerou debates sobre a proteção de dados pessoais em várias partes do mundo. A criação do GDPR inspirou outras legislações, como a CCPA (Lei

de Privacidade do Consumidor da Califórnia) e a LGPD (Lei Geral de Proteção de Dados), no Brasil.

Princípios Fundamentais da Proteção de Dados Pessoais

De acordo com o GDPR, ao tratar dados pessoais, as organizações devem seguir uma série de princípios básicos para garantir que o processo seja justo e transparente (União Europeia, 2016). Esses princípios incluem:

- a) **Licitude, lealdade e transparência:** As informações sobre o tratamento dos dados devem ser claras, acessíveis, concisas e compreensíveis para os titulares, garantindo total transparência.
- b) **Adequação e limitação da finalidade:** Os dados pessoais devem ser coletados com uma finalidade específica e usados somente de maneira compatível com essa finalidade.
- c) **Necessidade e minimização:** Apenas dados essenciais para a finalidade do processamento devem ser coletados, evitando a coleta excessiva de informações.
- d) **Qualidade dos dados:** Os dados devem ser precisos, atualizados e não excessivos em relação às finalidades para as quais são tratados.
- e) **Limitação da conservação:** Os dados não podem ser retidos por mais tempo do que o necessário para cumprir a finalidade para a qual foram coletados.
- f) **Segurança, integridade e confidencialidade:** É imprescindível que as organizações assegurem que os dados pessoais sejam tratados de maneira segura, protegendo-os contra acessos não autorizados ou danos.
- g) **Prestação de contas:** As organizações devem ser capazes de demonstrar que estão cumprindo os requisitos do regulamento, implementando medidas adequadas para garantir a proteção dos dados pessoais.

Direitos dos Titulares de Dados Pessoais

O GDPR garante aos titulares dos dados uma série de direitos, permitindo-lhes assumir o controle sobre suas informações pessoais. A transparência é um dos

princípios centrais, exigindo que as empresas informem claramente a finalidade do uso dos dados e obtenham o consentimento explícito dos titulares para processá-los.

Entre os direitos dos titulares estão a possibilidade de retirar o consentimento a qualquer momento, retificar informações imprecisas, e até mesmo solicitar a exclusão definitiva de seus dados após o término da relação com a organização. Além disso, o titular tem o direito de limitar o tratamento de seus dados, especialmente se houver dúvidas sobre a precisão ou legalidade das informações.

De acordo com o Guia do Cidadão para a Proteção de Dados da Comissão Europeia (2019), os direitos dos titulares incluem:

- a) Direito à transparência das informações e regras para o exercício dos direitos dos titulares;
- b) Direito de acesso aos dados pessoais coletados;
- c) Direito de retificação e correção de dados imprecisos;
- d) Direito ao apagamento (também conhecido como "direito ao esquecimento");
- e) Direito de limitação do tratamento;
- f) Obrigação de notificação em casos de retificação, apagamento ou limitação do tratamento;
- g) Direito de portabilidade dos dados;
- h) Direito de oposição ao tratamento de dados;
- i) Direito sobre decisões automatizadas, incluindo a definição de perfis.
- j) Segurança dos Dados Pessoais

Para assegurar a proteção dos dados pessoais, o GDPR exige que as organizações adotem medidas técnicas e organizativas adequadas ao risco envolvido. Essas medidas devem considerar a natureza, o contexto e as finalidades do tratamento, bem como os riscos para os direitos e liberdades dos indivíduos.

Entre as medidas recomendadas estão:

- a) **Pseudonimização e cifragem:** A utilização de técnicas que tornam os dados mais difíceis de serem identificados ou acessados por terceiros não autorizados.

- b) **Anonimização:** Garantir que os dados não possam mais ser atribuídos a um titular específico sem o uso de informações adicionais.
- c) **Recuperação de dados:** As organizações devem ter planos para restaurar a disponibilidade e o acesso aos dados pessoais em caso de incidentes técnicos ou físicos.
- d) **Testes regulares:** Avaliações periódicas para garantir a eficácia das medidas de segurança adotadas.

Além disso, o regulamento exige que, em caso de violação de dados pessoais, os controladores de dados notifiquem a autoridade de proteção de dados competente em até 72 horas, a menos que a violação não represente risco para os direitos dos indivíduos. Também é necessário informar os titulares afetados o mais rápido possível.

Avaliação de Impacto sobre a Proteção de Dados (DPIA)

O GDPR exige que, quando um tratamento de dados pessoais representar um alto risco para os direitos dos indivíduos, especialmente no caso de uso de novas tecnologias, a organização realize uma Avaliação de Impacto sobre a Proteção de Dados (DPIA). Isso deve ser feito antes de iniciar qualquer operação de tratamento que possa representar riscos elevados.

De acordo com a Universidade de Coimbra (2017), a DPIA deve identificar e mitigar riscos antes de realizar o tratamento de dados e, em alguns casos, consultar as autoridades de proteção de dados se os riscos não puderem ser mitigados adequadamente.

4.1.3 CCPA (*California Consumer Privacy Act*)

A globalização, a popularização da internet e o surgimento de tecnologias como o aprendizado de máquina e a inteligência artificial transformaram as práticas de interação e socialização de dados. Tais inovações, embora tenham contribuído para a integração e facilitação das relações humanas, também aumentaram a criação, processamento, armazenamento e compartilhamento de dados, expondo os indivíduos a novas ameaças no universo digital.

Armando Junior (2020), em sua obra *Desafios Estratégicos para a Segurança e Defesa Cibernética*, aponta que, em um cenário de grande diversidade de redes e tecnologias, emerge um comportamento recorrente nas relações humanas: o uso indevido da internet para obter recursos de forma ilícita ou fraudulenta. Diante deste ambiente, onde coexistem tanto ameaças quanto medidas de defesa, os Estados têm buscado proteger suas infraestruturas e populações. Naturalmente, essa proteção envolve a defesa de interesses no espaço cibernético, voltada para a Segurança Nacional, com foco tático e operacional, inclusive na perspectiva da Guerra Cibernética.

Nesse contexto de transformação digital, surgiu a necessidade de novas abordagens para garantir o direito à privacidade dos dados, oferecendo aos indivíduos maior controle sobre o uso de suas informações pessoais.

A *California Consumer Privacy Act* (CCPA), ou Lei de Privacidade do Consumidor da Califórnia, é uma legislação que visa estabelecer direitos significativos para os residentes californianos, garantindo-lhes maior controle sobre suas informações pessoais. Além de sua aplicação em território californiano, a CCPA possui caráter extraterritorial, o que significa que empresas que tratem dados de residentes da Califórnia estão sujeitas a suas disposições, independentemente de sua localização.

Inspirada na *General Data Protection Regulation* (GDPR) da União Europeia, a CCPA reflete os esforços para proteger os dados pessoais e a privacidade dos consumidores em uma região globalmente reconhecida como um centro de inovação tecnológica. A Califórnia, sede do Vale do Silício, onde estão localizadas gigantes como Facebook e Apple, tem exercido influência sobre outras jurisdições, sendo pioneira na regulamentação sobre a notificação de vazamentos de dados, prática adotada por todos os 50 estados dos Estados Unidos.

Sancionada em 2018, a CCPA entrou em vigor em janeiro de 2020, abrangendo consumidores, famílias e domicílios residentes no Estado (DEPARTAMENTO DE JUSTIÇA DO ESTADO DA CALIFÓRNIA, 2018). A legislação californiana define como residentes do estado não apenas aqueles que residem permanentemente na Califórnia, mas também aqueles que se encontram temporariamente fora do Estado por motivos não transitórios.

Princípios Fundamentais da Proteção de Dados Pessoais

A CCPA aplica-se a empresas de qualquer parte do mundo que processem dados pessoais de consumidores residentes na Califórnia, com fins lucrativos, nas seguintes situações:

Quando comprem, vendem ou compartilham dados pessoais para fins comerciais;

Quando excedem certos limites, como tratar dados de mais de 50.000 residentes, ter 50% de sua receita proveniente da venda de dados pessoais ou atingir uma receita bruta anual superior a US\$ 25 milhões.

A CCPA estabelece penalidades significativas para o não cumprimento, incluindo multas que variam de US\$ 2.500 por violação a US\$ 7.500 para violações intencionais, caso a ofensa não seja corrigida dentro de 30 dias após a notificação da violação. A fiscalização é realizada pelo procurador-geral da Califórnia. Além disso, os consumidores têm o direito de buscar compensações financeiras através de ações judiciais, com a possibilidade de obter danos estatutários entre US\$ 100 a US\$ 750 por consumidor ou indenizações por danos concretos, se comprovar perdas financeiras decorrentes de acesso indevido a dados não criptografados.

As empresas infratoras têm um prazo de 30 dias após a notificação para corrigir a violação. Caso contrário, o titular pode buscar a compensação judicialmente.

Direitos dos Titulares de Dados Pessoais

A CCPA concede aos titulares dos dados uma série de direitos, com destaque para a possibilidade de optar por não permitir a venda de suas informações pessoais. As empresas são obrigadas a respeitar essa decisão, garantindo aos consumidores maior controle sobre como suas informações são tratadas. A regulamentação californiana reflete, assim, uma abordagem robusta de proteção à privacidade, alinhando-se aos direitos dos indivíduos em um cenário global cada vez mais digitalizado e interconectado.

4.2 Análise Comparativa das Normativas de Proteção de Dados

A comparação entre a LGPD e o GDPR revela tanto semelhanças quanto diferenças significativas, principalmente no que tange à proteção dos dados pessoais e aos direitos dos consumidores. Ambas as legislações exigem o consentimento

explícito para a coleta e o processamento de dados pessoais, assegurando direitos como acesso, retificação e eliminação dessas informações.

No entanto, há distinções notáveis na abrangência e na aplicação das normas. O GDPR é aplicável globalmente a qualquer empresa que trate dados de cidadãos da União Europeia, independentemente de sua localização, enquanto a LGPD se aplica a empresas que lidam com dados pessoais no Brasil, independentemente da localização geográfica. Já a CCPA é mais restrita, aplicando-se apenas aos consumidores da Califórnia e adotando um modelo flexível de "*opt-out*" (direito de não ser incluído na coleta de dados), em contraste com o modelo de "*opt-in*" exigido pelo GDPR e pela LGPD, que requer consentimento explícito para a coleta de dados.

O Regulamento Europeu de Proteção de Dados Pessoais (GDPR) desempenhou um papel fundamental ao estimular outros países a adotarem legislações específicas para a proteção da privacidade e dos dados pessoais. Após sua implementação, a Califórnia seguiu esse exemplo, criando o *California Consumer Privacy Act* (CCPA), em 2018, com a entrada em vigor em janeiro de 2020. Essa lei foi uma resposta à necessidade de proteger os dados dos residentes californianos e garantiu novos direitos em relação à privacidade. Seguindo esse movimento, o Brasil promulgou a Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020 e trouxe consigo medidas para a proteção dos dados pessoais no país.

No Brasil, as sanções por descumprimento da LGPD começaram a ser aplicadas em agosto de 2021, com penalidades que podem chegar a 2% do faturamento da empresa, limitadas a R\$ 50 milhões por infração. Essas sanções visam promover a conformidade e assegurar que as empresas tratem os dados pessoais de maneira responsável e transparente.

Embora essas legislações apresentem diferenças de acordo com as particularidades de cada região, elas compartilham objetivos semelhantes, principalmente no que diz respeito à proteção dos dados pessoais. As leis destacam princípios fundamentais como transparência, consentimento explícito e direitos de revogação e atualização dos dados pelos titulares. Esses princípios garantem que os indivíduos tenham o controle sobre suas informações pessoais e possam gerenciá-las conforme suas preferências.

Além disso, no Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) desempenha um papel fundamental, não apenas regulando e fiscalizando, mas também promovendo a conscientização das organizações sobre a importância da proteção de dados. Em caso de descumprimento, a ANPD pode aplicar advertências, estabelecendo prazos para que as empresas adotem medidas corretivas, antes de aplicar sanções mais rigorosas, conforme previsto na LGPD. A legislação brasileira ainda prevê a aplicação de multas, bloqueio, eliminação de dados pessoais e a divulgação da infração, a fim de assegurar o cumprimento das normas estabelecidas. Além disso, a ANPD também desenvolve resoluções complementares para garantir a implementação eficaz da LGPD.

Em relação à GDPR, a legislação europeia é rigorosa quanto à aplicação de sanções. Empresas que violam as normas podem ser penalizadas com multas de até 20 milhões de euros ou 4% da receita global anual (o que for maior). As sanções podem variar dependendo da gravidade e da duração da infração, e cada país da União Europeia tem sua autoridade reguladora, que colabora com as demais para garantir que a conformidade seja mantida em todo o território da União. Além disso, o GDPR também exige que as empresas realizem uma avaliação de impacto à proteção de dados pessoais quando o tratamento de dados puder representar um alto risco para os direitos e liberdades dos indivíduos, especialmente em casos de tratamento automatizado ou de grandes volumes de dados sensíveis.

As sanções e a cooperação entre as autoridades de proteção de dados são fundamentais para garantir a eficácia das legislações e promover um ambiente em que as empresas e os consumidores possam confiar na proteção de suas informações pessoais. A adesão a boas práticas de autorregulação, como a adoção de códigos de conduta e certificações, também contribui para a construção de um mercado mais transparente e responsável em relação à privacidade.

Essas diferenças legislativas têm implicações diretas nas práticas de comercialização de dados pessoais realizadas pelos *data brokers*, que devem adotar políticas sólidas de transparência, responsabilidade e governança no tratamento dessas informações. Além disso, torna-se essencial o fortalecimento da fiscalização e a implementação de mecanismos eficazes de governança de dados, a fim de assegurar a conformidade com os marcos regulatórios e preservar os direitos dos titulares em um ambiente digital cada vez mais complexo e sensível à privacidade.

4.3 O Papel dos *Data brokers* nas Normativas de Proteção de Dados

O fenômeno crescente dos *data brokers* (corretores de dados) tem sido uma das principais preocupações para o fortalecimento das legislações de proteção de dados, como o GDPR, a LGPD e a CCPA. A evolução das normas de proteção de dados tem como objetivo criar barreiras legais e regulatórias que impeçam abusos por parte dessas empresas e promovam a transparência no uso de informações pessoais.

No contexto do GDPR, a abordagem visa garantir que os dados coletados por terceiros, nesse contexto, como os *data brokers*, sejam tratados de forma justa e com o consentimento adequado do titular dos dados. A legislação impõe obrigações de transparência e controle ao exigir que os consumidores tenham acesso claro e simples sobre o que está sendo coletado, como é utilizado e por quem, além de assegurar o direito de retirada dos dados.

A LGPD, em conformidade com o GDPR, também busca proteger os cidadãos brasileiros de práticas invasivas, impondo limites ao compartilhamento de dados pessoais sem consentimento explícito. A regulamentação dos *data brokers* no Brasil é uma área em crescente desenvolvimento, e os desafios para garantir o compliance dessas empresas são evidentes, considerando a natureza complexa e a diversidade das operações desses agentes no mercado global.

Na Califórnia, a CCPA oferece direitos adicionais para os consumidores, como a possibilidade de *opt-out* para a venda de seus dados pessoais. Isso implica que os consumidores possam escolher ativamente se desejam ou não permitir a comercialização de seus dados por *data brokers*, estabelecendo uma diferença significativa em relação a legislações que exigem o consentimento prévio (*opt-in*).

Embora essas legislações tragam avanços significativos, o impacto dos *data brokers* ainda representa uma das maiores ameaças à privacidade digital. A constante evolução das normativas, especialmente em termos de regulamentação do comércio de dados pessoais, é essencial para mitigar os riscos associados ao uso indevido e à comercialização descontrolada desses dados.

A transparência e o controle efetivo por parte dos indivíduos permanecem os principais pilares das leis de proteção de dados, buscando reduzir a assimetria de poder entre as empresas que coletam dados e os consumidores cujas informações estão sendo processadas.

4.4 A Conformidade dos Corretores de Dados com a Lei Geral de Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018) impacta diretamente os corretores de dados que exploram informações de cidadãos brasileiros ou que operam atividades de tratamento de dados pessoais no Brasil. Não é por acaso que várias empresas atuando como corretoras de dados no país já adotaram um discurso "pró-LGPD" e buscam afirmar conformidade com a legislação. No entanto, a implementação plena e eficaz da LGPD em sua aplicação aos corretores de dados é um desafio complexo que envolve uma série de aspectos jurídicos, comerciais e éticos.

Discutem-se três aspectos centrais da aplicabilidade da LGPD aos corretores de dados: a) o problema das bases legais para o tratamento de dados; b) os deveres aplicáveis aos corretores de dados, considerando o intercruzamento da LGPD com o Código de Defesa do Consumidor e a Lei do Cadastro Positivo; e c) a problemática do tratamento excessivo de dados, especialmente quando se torna impossível para o titular conhecer ou contestar um dado inferencial, originado a partir do cruzamento de suas informações pessoais em um tratamento prévio.

4.4.1 O Problema das Bases Legais para o Tratamento de Dados

A questão das bases legais (*legal grounds for data processing*) não é nova no debate sobre a aplicabilidade dos direitos de proteção de dados ao mercado dos corretores de dados. No relatório publicado em 2006 pela Clínica Canadense de Política e Interesse Público da Internet (CIPPIC), foi identificado que, frequentemente, os corretores de dados fornecem respostas semelhantes quando questionados sobre a licitude de suas práticas. Uma das respostas mais comuns é a alegação de que os dados são "tratados com consentimento" (CIPPIC, 2006). Contudo, é necessário analisar qual tipo de consentimento é realmente dado, uma vez que, dada a opacidade característica desse mercado, raramente são atendidas as especificidades exigidas no artigo 5º, XII, da LGPD, que define o consentimento como sendo livre, informado e inequívoco, destinado a uma finalidade específica.

Caso as informações fornecidas aos titulares sejam enganosas ou abusivas, desrespeitando as exigências legais, isso poderá invalidar o consentimento dado. Em

um relatório mais recente, de 2020, oriundo de uma investigação do *Information Commissioner Office* (ICO) contra empresas como *Experian*, *Equifax* e *TransUnion*, ficou claro que é essencial que a base legal para o tratamento de dados seja clara, e que os dados oferecidos estejam em conformidade com as exigências da proteção de dados antes de qualquer serviço de corretagem ser executado. A investigação revelou falhas sistêmicas de proteção de dados em todo o setor, destacando a importância de princípios como transparência, justiça e legalidade na coleta e uso de dados pessoais (ICO, 2020).

Entretanto, muitos corretores de dados atualmente se amparam em outra base legal: o legítimo interesse, conforme o artigo 7º, XI, da LGPD. Esta base tem gerado consideráveis discussões jurídicas, uma vez que sua aplicação exige um balanceamento entre o interesse legítimo de quem realiza o tratamento e as expectativas dos titulares de dados. Para utilizar essa base de forma adequada, deve ser realizado um "Teste de Legítimo Interesse" (*Legitimate Interests Assessment - LIA*), que deve ser documentado conforme as exigências da LGPD (ANPD, 2020).

Assim, a simples alegação de que o tratamento de dados está amparado pelo legítimo interesse não é suficiente; é necessário demonstrar, por meio de documentação adequada, que o processo respeita a legalidade e os direitos dos titulares. A Autoridade Nacional de Proteção de Dados (ANPD) também pode solicitar relatórios sobre o impacto à proteção de dados pessoais, o que pode levar à revisão da operação (ANPD, 2020).

A aplicação do legítimo interesse no contexto da Lei Geral de Proteção de Dados (LGPD) reflete uma adaptação do modelo europeu, principalmente ao considerar a flexibilidade dessa base legal, que permite uma ampla gama de usos para os dados pessoais. A base legal do legítimo interesse, conforme previsto no Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, tem ganhado destaque principalmente pela sua aplicabilidade em cenários onde outras bases legais, como o consentimento, seriam difíceis de aplicar (Bioni, 2019). Contudo, como a definição de "interesse" no contexto do tratamento de dados continua sendo um tema controverso e de amplo debate, uma vez que, embora a lei ofereça um conceito, este não é totalmente claro.

Maziero e Silva (2021, p. 23-25), abordam que a legislação europeia buscou estabilizar a aplicação do conceito jurídico de legítimo interesse, tratando-o como um

ponto de equilíbrio entre os titulares dos dados, os agentes reguladores e as partes envolvidas na cadeia de tratamento de dados. O objetivo central dessa abordagem é garantir previsibilidade na aplicação da base legal do legítimo interesse. Nesse sentido, é importante destacar os considerandos 47, 48 e 49 do Regulamento (UE) 2016/679 (GDPR), que fornecem diretrizes sobre a utilização dessa base legal.

De acordo com os entendimentos presentes nos considerandos do Regulamento (UE) 2016/679, o simples fato de o responsável pelo tratamento de dados pessoais possuir um interesse legítimo não é suficiente para justificar a aplicação da base legal prevista no artigo 6º, alínea (f) do GDPR. É necessário realizar uma análise mais aprofundada, considerando outros fatores destacados nos referidos considerandos. Por exemplo, pode ser considerado legítimo quando há uma relação prévia entre a pessoa e a empresa, como no caso de clientes ou funcionários. Ainda assim, é necessário avaliar cuidadosamente se o titular dos dados poderia prever esse uso no momento em que os dados foram coletados.

Além disso, a legislação destaca que certas situações específicas – como a prevenção à fraude, a segurança de redes e sistemas ou o compartilhamento interno de dados dentro de um grupo empresarial – também podem justificar o uso do legítimo interesse, desde que sejam respeitados os princípios de necessidade e proporcionalidade.

Maziero e Silva (2021) ressalta que o simples fato de a empresa ou organização ter um interesse legítimo não é suficiente para justificar o tratamento. É preciso aplicar o chamado teste tríplice, que avalia três pontos:

1. Qual é o interesse legítimo envolvido (teste da finalidade);
2. Se o tratamento dos dados é realmente necessário para atingir esse interesse (teste de necessidade);
3. Se os direitos e liberdades dos titulares são respeitados diante desse interesse (teste de proporcionalidade).

Esse equilíbrio é essencial para garantir que o tratamento de dados com base no legítimo interesse seja feito de forma ética, transparente e em conformidade com a LGPD.

O legítimo interesse, portanto, deve ser cuidadosamente balanceado com os direitos dos titulares, e isso implica realizar um “Teste de Legítimo Interesse” (LIA), como previsto pela LGPD, para garantir que o tratamento de dados seja legítimo e

transparente. Dessa forma, é essencial que empresas que adotam essa base legal considerem não apenas os seus próprios interesses, mas também as implicações sociais e os direitos dos indivíduos envolvidos.

4.5 Os Deveres Aplicáveis aos Corretores de Dados e o Princípio da Boa-Fé

Em 2014, o julgamento do Recurso Especial 1.419.697/RS, na primeira audiência pública da história do Superior Tribunal de Justiça (STJ), consolidou o entendimento sobre a natureza dos sistemas de *scoring* e as possíveis violações ao Código de Defesa do Consumidor (CDC), com implicações sobre a responsabilidade por danos morais. O julgamento reconheceu que a utilização do sistema de pontuação de crédito, embora lícita, deve ser realizada com transparência e boa-fé na relação com os consumidores, e que qualquer violação aos limites legais nesse processo pode resultar em abuso de direito e, conseqüentemente, em responsabilidade objetiva e solidária das partes envolvidas.

Esse precedente serve como um importante marco para a atividade de corretagem de dados, já que destaca a necessidade de respeitar princípios fundamentais, como veracidade, clareza, transparência e a não utilização de informações excessivas ou sensíveis. A boa-fé, nesse contexto, é um princípio central que orienta a aplicação da LGPD aos corretores de dados. De acordo com o artigo 6º da LGPD, o tratamento de dados pessoais deve ser realizado de acordo com os princípios da boa-fé, vedando que ele seja feito com fins discriminatórios, ilícitos ou abusivos. Isso significa que as corretoras de dados devem operar dentro de parâmetros éticos e legais, garantindo a confiança dos titulares no uso de suas informações.

O princípio da boa-fé objetiva também se relaciona diretamente com a necessidade de garantir a segurança das informações pessoais. A responsabilidade das empresas de corretagem de dados não se limita à coleta de dados, mas também à proteção e ao uso adequado das informações, sendo que os titulares devem poder confiar que seus dados serão tratados de maneira segura e transparente.

4.6 O Tratamento Excessivo de Dados e a Proteção dos Direitos Fundamentais

Outro ponto crítico relacionado aos corretores de dados diz respeito ao tratamento excessivo de dados. Isso ocorre quando o volume de dados coletados ou a forma como são utilizados extrapola o necessário para a finalidade de uma determinada atividade comercial, comprometendo a privacidade e a autodeterminação informativa dos titulares. A LGPD estabelece que os dados pessoais devem ser tratados de forma adequada, relevante e limitada ao necessário para as finalidades para as quais são coletados, conforme o princípio da minimização de dados (art. 6º, §1º).

Em um mercado que já sofre com a assimetria informacional, onde os titulares de dados muitas vezes não têm conhecimento sobre como suas informações são compartilhadas e utilizadas, a necessidade de transparência e de controle sobre os dados pessoais se torna ainda mais urgente. O direito à oposição, conforme o artigo 18, §2º, da LGPD, deve ser garantido, permitindo que os titulares se oponham ao tratamento de seus dados, especialmente quando realizado com base no legítimo interesse.

Por fim, é essencial que os corretores de dados, ao atuarem no mercado, respeitem as limitações e os parâmetros éticos estabelecidos pela LGPD, para que não haja a exploração indevida de dados pessoais, especialmente quando esses dados são usados para práticas discriminatórias ou abusivas, como o perfilamento preditivo que resulta em categorias sociais e comerciais prejudiciais aos indivíduos.

A conformidade dos corretores de dados com a LGPD é, portanto, essencial para garantir que a coleta e o tratamento de dados pessoais sejam feitos de maneira justa, transparente e respeitosa aos direitos fundamentais dos indivíduos, promovendo a confiança do consumidor e a integridade do mercado digital.

4.7 Desafios Regulatórios e Compliance

4.7.1 Serasa Experian x MPDFT – Suspensão da Venda de Dados Pessoais e a Importância de Compreender a Atividade dos Data brokers na Economia de Dados

Um caso paradigmático que evidencia os desafios na aplicação prática da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) é a Ação Civil Pública ajuizada pelo Ministério Público do Distrito Federal e Territórios (MPDFT) em face da empresa Serasa S.A. (Serasa Experian), a qual tramitou sob o nº 0736634-

81.2020.8.07.0001, e teve como objeto a suspensão da comercialização de dados pessoais por meio dos produtos intitulados “Lista Online” e “Prospecção de Clientes” ofertados pela Serasa no mercado nacional.

Segundo o MPDFT, os serviços ofertados pela Serasa consistiam na disponibilização massiva de dados de aproximadamente 150 milhões de brasileiros, contendo informações como nome, número de CPF, endereço, telefone, perfil financeiro, poder aquisitivo, classe social e afinidades, comercializados por valores inferiores a R\$ 1,00 por indivíduo. Para o órgão ministerial, essa prática configura um grande incidente de segurança monetizável (BRASIL, 2021), incompatível com os princípios fundamentais da LGPD e da Constituição Federal, especialmente os relativos à privacidade, intimidade e autodeterminação informativa (CF, art. 5º, X; LGPD, art. 2º, I).

Em primeira instância, o juízo da 5ª Vara Cível de Brasília indeferiu o pedido de liminar. Contudo, ao analisar o Agravo de Instrumento nº 0749765-29.2020.8.07.0000, o Tribunal de Justiça do Distrito Federal e Territórios (TJDFT), por decisão monocrática do Desembargador Cesar Loyola, deferiu a tutela recursal para determinar a suspensão imediata da comercialização dos dados pessoais por parte da Serasa, sob pena de multa de R\$ 5.000,00 por transação (TJDFT, 2021).

A Serasa, cuja atividade define-se como um *data broker*, argumentou que os dados comercializados seriam de natureza não sensível, de caráter público ou cadastral, e obtidos legitimamente no contexto de relações civis e comerciais rotineiras. A empresa defendeu ainda que sua conduta estaria respaldada no legítimo interesse previsto no art. 7º, inciso IX da LGPD, que permite o tratamento de dados pessoais sem consentimento quando necessário para atender interesses legítimos do controlador, desde que respeitados os direitos e liberdades fundamentais do titular.

Contudo, o Tribunal afastou essa justificativa ao afirmar que o legítimo interesse não é autorização genérica para o tratamento indiscriminado de dados, especialmente quando há comercialização remunerada de dados pessoais entre controladores com finalidade de marketing. Destacou-se que, salvo se os dados forem tornados manifestamente públicos pelo próprio titular, a regra geral da LGPD exige consentimento informado e específico para cada finalidade (LGPD, art. 7º, § 4º). Segundo Loyola (TJDFT, 2021), “*não se pode presumir que os dados foram tornados públicos de forma ampla e irrestrita a ponto de poderem ser comercializados*”.

A decisão também ressaltou que a prática fere os princípios da finalidade, necessidade e transparência, consagrados no art. 6º da LGPD, uma vez que os titulares não tinham conhecimento claro do uso que seria feito de seus dados. Como enfatiza Doneda (2021, p. 142), “o *legítimo interesse não pode ser invocado como uma carta branca para flexibilizar os direitos dos titulares, sobretudo quando se trata de relações assimétricas entre grandes corporações e indivíduos*”.

O caso ressalta a complexidade do conceito de legítimo interesse na coleta e tratamento de dados pessoais, especialmente quando a finalidade da coleta se altera. O tribunal de primeira instância argumentou que não havia necessidade de consentimento para a venda de dados, pois estes seriam habitualmente fornecidos nas relações negociais e empresariais, mas falhou em considerar a mudança de finalidade e os direitos dos titulares dos dados. Esse tipo de interpretação pode gerar conflitos em relação à Lei Geral de Proteção de Dados Pessoais (LGPD), que estabelece normas rigorosas para a coleta e comercialização de dados, incluindo a exigência de consentimento explícito para algumas finalidades, como marketing.

Além disso, a decisão também destaca uma lacuna significativa no entendimento do Poder Judiciário sobre a natureza dos *data brokers* e as bases legais para o tratamento de dados, o que reflete uma necessidade urgente de maior capacitação dos operadores do Direito no que diz respeito à aplicação da LGPD e à compreensão dos modelos de negócios das empresas que atuam na economia de dados.

Este caso coloca em evidência a atuação dos chamados *data brokers* agentes intermediários que coletam, organizam e comercializam dados pessoais como ativo econômico, cuja atividade deve ser rigidamente avaliada à luz da legislação brasileira de proteção de dados. A decisão do TJDF não apenas reforça o papel protetivo da LGPD, como também evidencia a necessidade de maior transparência, e responsabilidade por parte de empresas que operam com grandes volumes de dados.

4.7.2 A Proteção de Dados Pessoais e a Responsabilidade no Contexto do Credit Scoring

As raízes desta dissertação encontram-se não somente na análise abrangente da decisão do Superior Tribunal de Justiça (STJ) no caso paradigmático sobre *credit scoring*, mas também em decisões históricas que tratam dos direitos dos

consumidores e da proteção de dados pessoais. Uma dessas decisões é a de 1995, proferida pelo ministro Ruy Rosado Aguiar, que reconheceu a opressão econômica provocada pelo tratamento de dados pessoais sem a devida autodeterminação informativa dos consumidores. Este julgamento se configurou como uma base relevante para as discussões contemporâneas acerca da privacidade e da utilização de dados pessoais no contexto das práticas comerciais.

Em sua decisão, o ministro Ruy Rosado destacou a crescente preocupação do Estado moderno com o uso indiscriminado de informações pessoais. A utilização da informática, que possibilita o controle unificado das atividades pessoais, pode levar a uma invasão de privacidade, onde detalhes íntimos da vida do indivíduo podem ser conhecidos sem que o titular dos dados tenha consciência ou meios adequados de controle sobre suas informações. O voto do ministro, no caso que envolvia o Clube de Diretores Lojistas de Passo Fundo, é esclarecedor:

A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permite o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade. (Brasil. STJ, Recurso Especial n. 22.337-8/RS, Relator Ministro Ruy Rosado Aguiar, 1995)

Este caso foi pioneiro ao apontar para o risco de abuso que a falta de controle e transparência no tratamento de dados pessoais pode causar ao consumidor, sendo um marco inicial no reconhecimento da necessidade de uma maior regulação para proteger a privacidade. Em sua argumentação, o ministro ainda alertou sobre o uso potencialmente indevido das informações pessoais para fins contrários à moral e ao direito, como perseguição política ou opressão econômica.

A decisão de 1995 interage com a jurisprudência mais recente do STJ, como no Recurso Especial nº 1.758.799-MG, relatado pela ministra Nancy Andrighi. Em sua decisão, a ministra enfatizou os direitos do consumidor de tomar conhecimento das informações a seu respeito armazenadas por terceiros, mesmo sem sua autorização, e de ter acesso e poder de correção sobre essas informações. Esse entendimento reflete uma preocupação mais ampla com os direitos à autodeterminação informativa, que garante ao consumidor o controle sobre seus dados pessoais.

A ministra Andrighi assinalou que o tratamento inadequado de dados, seja por sua coleta indevida, armazenamento ou compartilhamento com terceiros, pode gerar danos materiais e imateriais, configurando, assim, a necessidade de reparação ao consumidor:

A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor – dentre os quais se inclui o dever de informar – faz nascer para este a pretensão de indenização pelos danos causados. (Brasil. STJ, Recurso Especial nº 1.758.799-MG, Relatora Ministra Nancy Andrighi, 2019)

Além disso, a ministra apontou que, em contextos como o da empresa Procob, que atuava como corretora de dados, é fundamental que haja transparência quanto ao uso das informações. O consumidor, ao ser cadastrado em sistemas como o Cadastro Positivo, tem o direito de ser informado sobre a identidade do gestor dos dados e os objetivos para os quais seus dados estão sendo tratados (Lei nº 12.414/2011, Art. 5º, V). Essa reflexão sobre a necessidade de informar os consumidores sobre o tratamento de seus dados pessoais se alinha diretamente ao princípio da transparência da Lei Geral de Proteção de Dados Pessoais (LGPD).

Uma das questões centrais que surgiram a partir do julgamento do Recurso Especial nº 1419697/RS, também conhecido como caso de *credit scoring*, está relacionada ao uso de dados excessivos ou sensíveis para a construção de perfis de crédito, prática que, de acordo com o STJ, pode violar os direitos do consumidor e exigir reparação. A decisão foi clara ao afirmar que, embora a prática de avaliação de risco de crédito (*credit scoring*) seja lícita, ela deve ser realizada dentro dos limites estabelecidos pela legislação, respeitando o direito à privacidade e à transparência nas relações de consumo:

O desrespeito aos limites legais na utilização do sistema 'credit scoring', configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consultante... (Brasil. STJ, Recurso Especial nº 1419697/RS, Relator: Ministro Paulo de Tarso Sanseverino, 2014).

A aplicação do sistema de "*credit scoring*" deve respeitar a privacidade do consumidor, evitando a utilização de informações excessivas ou sensíveis que não sejam diretamente relacionadas à análise do risco de crédito. A decisão do STJ

também previu que, no caso de descumprimento dos limites legais, a responsabilidade pelo uso indevido dos dados é objetiva e pode gerar reparação por danos morais ao consumidor.

Além disso, o tratamento de dados pessoais, especialmente quando envolve informações excessivas ou sensíveis, pode levar à violação dos direitos da personalidade, um ponto que foi amplamente discutido em outras decisões do STJ. A teoria do dano moral "*in re ipsa*" — ou seja, o reconhecimento de danos que são evidentes e independem de prova específica de prejuízo — foi aplicada nesses casos, especialmente em situações que envolvem a violação de direitos fundamentais como a privacidade (Brasil. STJ, Recurso Especial nº 640.196 PR, Relator: Ministro Castro Filho, 2005).

Por fim, ao analisar a interseção entre a proteção de dados pessoais e os direitos do consumidor, é possível perceber a necessidade de um modelo jurídico que não se limite à compensação de danos, mas que se foque na remoção do ilícito e na tutela específica do direito à privacidade. O sistema jurídico brasileiro, amparado pela LGPD e pela Constituição, oferece caminhos para a responsabilização de quem trata indevidamente os dados pessoais, sendo essencial que as empresas e instituições cumpram com seus deveres de transparência, informação e respeito aos direitos dos consumidores. Nesse contexto, a atuação preventiva e a tutela inibitória devem ser priorizadas, minimizando a ocorrência de danos e criando um ambiente mais seguro para o tratamento de dados pessoais.

4.8 Implementação de Compliance e a Governança no Setor Privado

A implementação das normas de proteção de dados apresenta desafios significativos para as empresas, que devem adaptar seus processos para atender às exigências de conformidade. Entre os principais desafios estão a adequação às novas legislações, a criação de políticas internas de governança e segurança de dados, e a capacitação de equipes para garantir que as práticas de coleta, armazenamento e uso de dados estejam em conformidade com as leis.

As empresas enfrentam desafios substanciais para cumprir as exigências da LGPD, do GDPR e de outras normativas internacionais, particularmente em relação à governança de dados. A conformidade regulatória exige investimentos significativos na criação de políticas internas e processos de compliance que garantam que a coleta

e o processamento de dados estejam alinhados com as exigências legais. Para os *data brokers*, esse desafio é ainda mais complexo devido à manipulação de grandes volumes de dados, muitas vezes sem o consentimento explícito dos indivíduos.

A governança de dados torna-se, nesse contexto, elemento central. Segundo o Data Governance Institute (DGI), trata-se de um sistema estruturado de decisões e responsabilidades sobre os processos que envolvem o uso da informação, baseado em modelos que determinam quem pode acessar e utilizar os dados, em que circunstâncias, com quais métodos e com que finalidade. De forma semelhante, Olavsrud (2020) define a governança de dados como o sistema organizacional que estabelece a autoridade e o controle sobre os ativos de dados, integrando pessoas, processos e tecnologias voltadas à sua gestão e proteção eficaz.

No âmbito organizacional, a governança corporativa também desempenha um papel estratégico. Segundo o Instituto Brasileiro de Governança Corporativa (IBGC, 2021), trata-se do sistema pelo qual empresas e demais organizações são dirigidas, monitoradas e incentivadas, abrangendo os relacionamentos entre sócios, conselhos de administração, diretorias, órgãos de fiscalização e controle, além das demais partes interessadas.

É essencial que a governança corporativa assegure que todas as práticas relacionadas à coleta, armazenamento, processamento e compartilhamento de dados pessoais estejam em conformidade não apenas com a legislação vigente, mas também com os princípios éticos, de responsabilidade e de transparência. A aplicação desses princípios fortalece a confiança da sociedade nas organizações, contribuindo para um ambiente digital mais seguro e íntegro.

Um conjunto de princípios fundamentais deve orientar as práticas de governança nas organizações, servindo como base para decisões éticas, transparentes e responsáveis. Entre eles, estão: capacidade de resposta, que representa a habilidade da instituição de reagir de forma ágil e eficaz às demandas e transformações do ambiente; integridade, que assegura condutas éticas e alinhadas aos valores organizacionais; transparência, indispensável para garantir clareza nas decisões e no uso das informações; equidade e participação, que promovem justiça, inclusão e envolvimento de todas as partes interessadas; *accountability* (prestação de contas), que estabelece a responsabilização pelos atos e decisões tomadas; confiabilidade, essencial para assegurar a segurança e consistência na gestão dos

dados; e, por fim, melhoria regulatória, voltada ao aperfeiçoamento contínuo das práticas e normas internas, acompanhando as inovações tecnológicas e exigências legais. Esses princípios fortalecem a legitimidade e a confiança da sociedade nas organizações, especialmente no tratamento responsável de dados pessoais.

Para consolidar essa cultura organizacional voltada à conformidade e à ética no tratamento de dados, é indispensável investir em programas de capacitação contínua, que promovam a conscientização dos colaboradores sobre os riscos e as obrigações legais associadas ao uso de dados pessoais. Tais iniciativas reforçam o compromisso da organização com a proteção dos direitos dos titulares de dados e com a construção de uma sociedade digital mais justa e transparente. Portanto, a adoção de boas práticas de compliance e governança de dados no setor privado é fundamental para consolidar a integridade das operações empresariais e promover um ambiente digital mais seguro, ético e competitivo.

4.8.1 Riscos Legais e Penalidades no Comércio de Dados Pessoais

O comércio de dados pessoais, especialmente por intermediários como os *data brokers*, envolve riscos legais significativos, incluindo multas e penalidades por violações das legislações de proteção de dados. As empresas devem estar atentas às obrigações legais para evitar sanções, que podem incluir multas substanciais, danos à reputação e processos judiciais. A conformidade é essencial para proteger tanto os dados dos consumidores quanto a integridade da organização.

A comercialização de dados pessoais sem o devido consentimento ou em desacordo com as normas de privacidade pode resultar em penalidades severas para as empresas na esfera administrativa e judicial. As sanções incluem multas substanciais, como as previstas pelo GDPR, que podem chegar a até 4% da receita anual global ou 20 milhões de euros, o que for maior. A LGPD, por sua vez, estabelece multas de até 2% da receita de uma empresa no Brasil, com um limite de 50 milhões de reais por infração. Essas penalidades têm como objetivo coibir práticas abusivas e garantir que as empresas adotem uma postura responsável no tratamento dos dados pessoais.

Casos judiciais, como o envolvendo a Google sob o GDPR, ilustram as implicações jurídicas para empresas que violam as normas de proteção de dados. A pressão regulatória crescente reflete um ambiente jurídico em que as empresas

devem não apenas se adequar às leis, mas também adotar práticas proativas de proteção de dados para evitar litígios e preservar sua reputação corporativa.

Os *data brokers* e empresas que os contratam devem desenvolver processos de governança de dados robustos e garantir que suas práticas de coleta e comercialização de dados estejam em conformidade com as legislações, como o GDPR, a CCPA e a LGPD. A conformidade com as obrigações contratuais e as responsabilidades legais em caso de descumprimento exige uma atenção constante às exigências regulatórias.

A violação das normas de privacidade pode resultar em penalidades severas, incluindo multas substanciais e danos à reputação. Empresas que não cumprirem as exigências legais enfrentarão consequências jurídicas significativas, como exemplificado pelos casos envolvendo grandes corporações no âmbito do GDPR. O mercado de dados está cada vez mais regulado, e a conformidade é essencial para evitar riscos legais e preservar a confiança do consumidor.

4.9 Desafios Éticos e Sociais na Comercialização de Dados Pessoais

Além dos aspectos legais, a comercialização de dados pessoais levanta questões éticas e sociais significativas, com impactos diretos sobre a privacidade dos indivíduos e a equidade no mercado digital. A centralização de dados e a personalização de serviços são práticas que geram preocupações sobre monopólios digitais e discriminação algorítmica.

Embora legislações como o GDPR e a LGPD busquem garantir que o consentimento seja livre, explícito e informado, a realidade é que muitos consumidores não compreendem completamente as implicações do uso de seus dados pessoais. A complexidade do tratamento de dados e a falta de transparência nas práticas dos *Data brokers* aumentam a vulnerabilidade dos indivíduos, dificultando a fiscalização das normas de privacidade.

Os impactos sociais da comercialização de dados podem ser profundos, como no caso da discriminação algorítmica, onde modelos automatizados de decisão podem negar o acesso a serviços financeiros, seguros ou até mesmo a oportunidades de emprego com base em perfis de risco. Tais práticas podem acentuar desigualdades sociais e econômicas, afetando desproporcionalmente grupos mais vulneráveis.

Portanto, a responsabilidade social das empresas não se limita ao cumprimento da legislação. Elas devem adotar práticas transparentes que respeitem os direitos dos consumidores e promovam o uso ético e justo dos dados pessoais. Isso inclui iniciativas educativas que ajudem os consumidores a compreender como seus dados são utilizados e como podem tomar medidas para proteger sua privacidade no ambiente digital.

Em um mundo cada vez mais digital e interconectado, a regulamentação e os aspectos legais envolvidos na comercialização de dados pessoais desempenham um papel crucial na proteção dos direitos dos consumidores e na criação de um mercado mais ético e transparente. Embora legislações como a LGPD, o GDPR e a CCPA representem avanços importantes, os desafios relativos à sua implementação, fiscalização e adaptação às rápidas inovações tecnológicas ainda são consideráveis.

Para os *data brokers*, o futuro será moldado pela necessidade de garantir uma conformidade rigorosa com essas normas, assegurando não apenas a conformidade legal, mas também um compromisso contínuo com a responsabilidade social e ética no uso de dados pessoais.

4.9.1 Ética Corporativa e Responsabilidade Social

A ética e o reconhecimento das responsabilidades em relação às comunidades atendidas por empresas, tanto públicas quanto privadas, são essenciais para definir o propósito organizacional, estabelecer um conjunto comum de valores, adotar métodos consistentes de tomada de decisão e fortalecer a confiança entre os usuários. A ética também desempenha um papel vital na reputação, no crescimento e na construção da marca das empresas. O desenvolvimento de uma estrutura ética corporativa permite que as empresas demonstrem como os dados confiados a elas são utilizados de maneira responsável, além de proporcionar flexibilidade para alinhar e atualizar continuamente as práticas empresariais, à medida que o desenvolvimento tecnológico avança, abordando questões que vão além da mera conformidade legal.

O uso da ética como um quadro analítico e operacional reconhece que a legislação, por sua natureza, não cobre todas as situações (e nem deveria), permitindo que as estruturas éticas corporativas desempenhem um papel decisivo na avaliação e na tomada de decisões sobre o uso de dados e algoritmos. Isso se torna particularmente relevante em dois cenários:

Quando valores e interesses concorrentes precisam ser equilibrados, e a legislação não oferece uma resposta simples ou direta.

Quando é possível fazer mais do que o que é estritamente exigido pela legislação?

Neste último caso, a ética justifica e facilita a implementação de práticas corporativas adicionais que não decorrem de exigências legais, mas que permitem que as empresas sigam os valores que definiram e cumpram sua missão de maneira integral. Essas práticas podem incluir, entre outras, investimentos em programas sociais, compromisso com iniciativas de transparência e apoio a campanhas educacionais.

Além disso, a ética pode auxiliar as empresas a atender às expectativas e seguir as recomendações dos órgãos reguladores, promovendo um relacionamento mais saudável e produtivo com essas entidades. Ela oferece uma base sólida para um diálogo sustentável e contínuo com reguladores, especialmente no que diz respeito à regulamentação do uso de tecnologias emergentes, como algoritmos e inteligência artificial. Nesse contexto, a CNIL (Autoridade Francesa de Proteção de Dados) definiu a ética como um processo orientador para questões legais, considerando o padrão ético como um precursor do padrão legal.

As estruturas éticas corporativas são essenciais para a construção de uma plataforma de diálogo e colaboração, promovendo uma cultura de engajamento construtivo entre órgãos reguladores e organizações responsáveis, o que é fundamental para a governança eficaz no mundo digital.

4.9.2.Desafios Éticos da Personalização de Serviços e Preços

A personalização de serviços e preços com base em dados pessoais tem se tornado uma prática comum no mundo digital, alimentada por algoritmos avançados e técnicas de aprendizado de máquina. Embora a personalização possa melhorar a experiência do usuário e aumentar a eficiência dos serviços, ela também traz à tona questões éticas significativas, principalmente em relação à equidade e à transparência no uso dos dados.

a) Práticas discriminatórias e desigualdade:

Um dos principais desafios éticos da personalização é o risco de discriminação. Quando as empresas utilizam dados pessoais para oferecer serviços e preços sob medida, elas podem criar situações onde indivíduos são tratados de forma desigual com base em características como idade, gênero, histórico de compras ou localização geográfica. Por exemplo, algoritmos podem estabelecer preços dinâmicos que variam de acordo com o comportamento de compra de um usuário ou com sua disposição aparente a pagar, sem que isso seja explícito ou justificável. Em alguns casos, isso pode resultar em um tratamento injusto, onde consumidores de diferentes origens econômicas ou sociais são cobrados de maneira desproporcional.

b) Falta de consentimento explícito:

Outro aspecto ético importante diz respeito ao consentimento. A personalização de serviços e preços geralmente depende da coleta de grandes volumes de dados sobre os consumidores. Muitas vezes, os indivíduos não têm plena consciência do quão detalhadas e invasivas as informações coletadas são, e não têm controle total sobre como essas informações são usadas. Mesmo quando o consentimento é solicitado, ele pode ser obtido de forma vaga ou obscura, sem explicitar de maneira clara o impacto que o uso dos dados terá sobre o usuário. Isso levanta questões sobre a transparência e a autonomia dos consumidores em relação ao controle sobre suas próprias informações.

c) Impacto na confiança do consumidor:

O uso excessivo e às vezes opaco de dados pessoais pode afetar negativamente a confiança dos consumidores nas plataformas digitais. Quando os consumidores percebem que estão sendo manipulados por algoritmos que ajustam preços ou serviços com base em dados pessoais, a confiança na marca pode ser abalada. Isso pode levar à frustração dos consumidores, que sentem que estão sendo tratados como "dados" e não como indivíduos, sem uma real escolha ou voz no processo. A falta de confiança também pode desencorajar a utilização de determinados serviços, prejudicando a experiência digital.

d) Efeitos na equidade social:

A personalização excessiva de serviços e preços pode aprofundar as desigualdades sociais. Se o acesso a produtos e serviços for determinado pelo comportamento online ou pela capacidade de gastar mais, usuários com menor poder aquisitivo podem ser marginalizados, ficando excluídos de determinados benefícios ou preços mais acessíveis. Além disso, a personalização pode reforçar preconceitos implícitos presentes nos dados, perpetuando desigualdades preexistentes.

Portanto, os desafios éticos da personalização de serviços e preços não se limitam apenas à questão da privacidade, mas envolvem um conjunto de preocupações sobre a equidade, o consentimento e a confiança no ambiente digital. O uso ético dos dados exige uma reflexão profunda sobre como as empresas devem equilibrar a personalização com a proteção dos direitos dos consumidores e a promoção de uma sociedade digital mais justa e transparente.

4.10 O Impacto Social da Monopolização de Dados

A monopolização de dados é um fenômeno crescente na economia digital, onde um número reduzido de grandes empresas concentra uma quantidade significativa de dados pessoais dos usuários. Este processo pode ter profundos impactos sociais, tanto em termos de competição no mercado quanto na proteção da privacidade dos indivíduos.

A concentração de dados nas mãos de poucas plataformas digitais gera um ambiente propenso à criação de monopólios digitais. Grandes empresas, como Google, Facebook (Meta), Amazon e Microsoft, dominam o mercado global, possuindo uma vasta quantidade de dados sobre os comportamentos, preferências e interações dos usuários. Isso cria um ciclo de dependência, onde os consumidores se tornam cada vez mais dependentes dessas plataformas para uma variedade de serviços – de pesquisa online a redes sociais, comércio eletrônico e até serviços de nuvem.

a) Implicações para a concorrência:

Esse domínio de dados pode gerar barreiras significativas à entrada de novos competidores no mercado. Empresas menores ou startups, que não possuem acesso aos mesmos volumes de dados, enfrentam dificuldades em competir de forma justa com os gigantes digitais. A falta de acesso a dados essenciais limita sua capacidade de personalizar serviços, melhorar ofertas ou até mesmo inovar, resultando em uma

competição desigual. Esse cenário não só prejudica a inovação, mas também dificulta o surgimento de alternativas no mercado, fortalecendo ainda mais o controle de empresas dominantes.

b) Desigualdade no acesso e uso dos dados:

A monopolização de dados pode levar a uma desigualdade significativa no acesso e no uso das informações. Plataformas dominantes têm a capacidade de coletar, analisar e monetizar dados de uma forma que é virtualmente inacessível para outras empresas, criando um desequilíbrio que favorece grandes corporações em detrimento de consumidores e pequenos negócios. Esse controle excessivo sobre os dados pode também resultar em uma falta de opções para os consumidores, já que eles são constantemente direcionados para as mesmas plataformas dominantes.

c) Implicações para a privacidade:

Quando grandes empresas controlam vastos volumes de dados pessoais, surgem sérios riscos para a privacidade dos indivíduos. O uso não transparente de dados, sem o devido consentimento ou sem a possibilidade de controle por parte dos titulares, pode levar a abusos de privacidade. Além disso, a centralização de dados aumenta o risco de vazamentos de informações, já que um único ataque cibernético ou falha de segurança pode afetar milhões de usuários de uma vez. A falta de concorrência também pode resultar em uma menor pressão para que as empresas adotem práticas de proteção de dados mais rigorosas.

Portanto, o impacto social da monopolização de dados se reflete diretamente na concentração de poder no mercado digital, na desigualdade de acesso à informação e na erosão da privacidade dos indivíduos. O fortalecimento de monopólios digitais pode, assim, ter consequências duradouras, prejudicando tanto a competitividade quanto a confiança dos consumidores nas plataformas digitais.

5 IMPLICAÇÕES ECONÔMICAS E EMPRESARIAIS

5.1 Empresa e a Economia

As implicações econômicas e empresariais no contexto da economia digital, destacando a organização dos fatores de produção e os custos de transação que permeiam as atividades comerciais. A análise dos custos de produção e transação oferece uma visão clara de como as empresas operam no mercado atual, onde a eficiência na gestão desses custos é essencial para o sucesso competitivo. A interação entre os fatores de produção e as transações jurídicas que estruturam o funcionamento empresarial é crucial para compreender a complexidade das relações econômicas contemporâneas.

O processo de comercialização de dados pessoais por empresas pode ser compreendido como uma extensão dessa lógica. A coleta, o tratamento e a monetização de dados envolvem negociações, formalização de contratos e mecanismos de proteção jurídica, o que implica diretamente em custos de transação. Ao entender a economia da empresa neste contexto, torna-se possível analisar como os *data brokers* se posicionam nesse ecossistema, atuando tanto como facilitadores operacionais quanto como agentes que desafiam a regulação vigente.

A empresa pode ser analisada sob duas perspectivas complementares. Na perspectiva estática, ela é o conjunto organizado de recursos economicamente relevantes, trabalho, capital, terra, tecnologia e capacidade empresarial. Já na perspectiva dinâmica, a empresa se constitui como um conjunto de transações jurídicas e contratuais que viabilizam a organização e o funcionamento desses recursos. Essa distinção permite compreender como a atividade empresarial se articula simultaneamente nos planos econômico e jurídico.

Conforme destaca Eduardo Goulart Pimenta (2022), na obra *Estrutura Jurídica da Empresa na Era Digital*, a produção e distribuição de bens e serviços dependem da combinação de recursos econômicos e relações jurídicas. É praticamente inviável que um único indivíduo produza ou preste serviços de maneira eficiente utilizando apenas seus próprios meios. Embora isso seja fisicamente possível, seria mais oneroso e menos rentável do que a produção realizada coletivamente, com diferentes indivíduos ocupando posições específicas ao longo da cadeia produtiva.

A organização dos fatores de produção exige, portanto, uma série de transações jurídicas entre o empresário e os agentes econômicos envolvidos, os trabalhadores, proprietários de terra, investidores e fornecedores. Essas transações viabilizam o acesso, o uso e a remuneração dos recursos necessários para manter a atividade produtiva. Cada fator de produção exige uma recompensa, como salários, juros, renda ou lucros compondo os custos de produção da empresa. A esses custos somam-se os custos de oportunidade, ou seja, o valor de outras alternativas que o empresário renuncia ao decidir aplicar seus recursos em determinada atividade.

O empresário, para implementar sua atividade econômica, realiza transações jurídicas com os diversos agentes econômicos, como os empregados, fornecedores de capital, donos de terras e outros fornecedores de recursos essenciais para a produção. Essas transações são fundamentais para garantir o funcionamento contínuo da empresa e, por consequência, a produção de bens ou serviços.

A empresa, nesse sentido, realiza a combinação dos fatores de produção – trabalho, capital, terra, tecnologia e capacidade empresarial, mediante a celebração de contratos com os diversos agentes econômicos.

De acordo com José Paschoal Rossetti,

Do emprego desses cinco fatores de produção, de sua disponibilidade, de suas qualificações ou capacitações, das formas de sua mobilização e de sua interação resultam os padrões de atendimento das ilimitáveis necessidades individuais e sociais. (ROSSETI, 2018)

A eficiente organização desses recursos é a chave para otimizar a produção e garantir a satisfação das necessidades econômicas.

Pimenta (2022) afirma que os fatores de produção, como terra, trabalho e capital, precisam de um organizador – o empresário. Esse empresário é o responsável por garantir que todos os fatores de produção sejam direcionados para um objetivo comum: a produção e distribuição eficientes de bens ou serviços. Sem essa organização, os fatores de produção por si só não geram nada.

Em termos econômicos, a empresa também deve lidar com três categorias de custos: custos de produção, custos de oportunidade e custos de transação. Os custos de produção envolvem os pagamentos aos fatores produtivos, como salários, juros e aluguéis. Os custos de oportunidade, por sua vez, referem-se ao valor das alternativas que o empreendedor renuncia ao decidir investir tempo e recursos em uma determinada atividade empresarial.

Além dos custos de produção e oportunidade, a empresa também deve lidar com os custos de transação, conceito fundamental desenvolvido por Ronald Coase em 1937. Em seu artigo clássico *The Nature of the Firm*, Coase formula a teoria da firma ao indagar por que as empresas existem, considerando que os mercados já permitem a contratação livre entre agentes. A resposta, segundo ele, está na tentativa de reduzir os custos associados à utilização do mercado. Esses custos incluem a busca por informações, a negociação, a elaboração de contratos e a supervisão de seu cumprimento.

O mercado é o ambiente onde circulam os bens e serviços e acontecem as negociações e celebração de contratos entre fornecedores e entre consumidores. Mas para atuar diretamente no mercado, há logicamente os custos de transação e grande instabilidade. Em razão disso, depender exclusivamente do mercado para todas as trocas econômicas reduz a eficiência, já que em certos momentos haverá escassez de alguns dos fatores de produção, como, por exemplo, mão de obra ou uma matéria-prima especial.

Para Ronald Coase:

(...) firmas, como instituição de aprovisionamento para facilitar o fornecimento de bens e serviços nos mercados, são resultado da procura de mecanismos de redução dos custos de transação, custos estes incorridos para ir ao mercado oferecer ou procurar bens e serviços (...) (COASE, 1990, p. 40)

Assim, pode-se dizer que há duas opções para realizar negociações econômicas: (i) diretamente no mercado e (ii) organizando sociedades empresárias. A organização de sociedades empresárias é importante para diminuir os custos e riscos nas transações que recaem sobre o empreendedor, em razão das imperfeições e instabilidades típicas do mercado. Ronald Coase afirma que as firmas são:

(...) perhaps the most important adaptation to the existence of transaction costs (COASE, 1990, p. 40)

Na sociedade empresária, são criadas equipes organizadas de prestadores de serviços e fornecedores de recursos, sob a gestão e controle de um único empresário, o que implica em uma produtividade mais eficiente.

Os custos de transação não se referem à remuneração direta dos fatores de produção, mas sim ao esforço financeiro, temporal e jurídico necessário para realizar

e manter as transações contratuais que estruturam a atividade empresarial. O empreendedor, nesse contexto, não apenas organiza recursos produtivos, mas também administra uma rede jurídica complexa, composta por contratos com empregados, fornecedores, financiadores e outros agentes.

Portanto, compreender os custos de transação é fundamental para a análise da estrutura jurídica da empresa. Eles incluem recursos gastos na negociação, elaboração e execução de contratos, bem como na proteção de direitos de propriedade e no cumprimento de obrigações legais. Esses custos se tornam ainda mais relevantes quando se analisa a empresa como uma instituição econômica moldada por fundamentos jurídicos, cuja eficiência depende da gestão inteligente desses custos.

A partir dessa leitura, compreende-se que a empresa é tanto uma estrutura produtiva quanto uma estrutura jurídica de coordenação de recursos. A operação empresarial requer transações formais com empregados, financiadores, locadores de imóveis, fornecedores e outros agentes econômicos. Cada uma dessas interações demanda contratos, acordos e mecanismos jurídicos de proteção e execução, compondo os custos de transação da atividade empresarial.

No contexto da economia digital, essa análise ganha novo alcance. A organização e o tratamento de dados pessoais pelas empresas representam um novo fator de produção. Esses dados, como ativos econômicos, exigem transações jurídicas específicas para sua coleta, armazenamento, compartilhamento e comercialização. Assim, os custos de transação se estendem para novas áreas reguladas, especialmente em relação à proteção de dados pessoais.

Nesse cenário, surgem os *data brokers*, empresas especializadas na intermediação de dados, que operam mediante uma complexa rede de contratos com diversas partes, utilizando-se da inovação e de tecnologias. Ao mesmo tempo em que facilitam processos empresariais e marketing direcionado, essas empresas também desafiam o aparato normativo vigente, elevando os custos de transação em razão da necessidade de conformidade regulatória.

Portanto, entender a lógica econômica da empresa, com ênfase nos custos de transação, é fundamental para analisar as implicações da comercialização de dados pessoais. A partir da estrutura jurídica e econômica da empresa discutida neste capítulo, é possível interpretar as novas dinâmicas de mercado na era digital. Isso

também abre caminho para o desenvolvimento de modelos regulatórios que consigam equilibrar a busca pela eficiência econômica com a necessidade de proteger os direitos fundamentais dos indivíduos, especialmente no que se refere à privacidade e à proteção de dados.

5.2 A Empresa no Direito Privado

O Direito Comercial surgiu historicamente para regulamentar as atividades comerciais, atendendo às demandas práticas de uma economia em expansão. Com a Revolução Industrial, tornou-se necessário criar normas jurídicas específicas para regular a crescente complexidade das práticas comerciais, que não podiam mais ser tratadas pelas normas do Direito Civil. No Brasil, a transição do conceito de "atos de comércio" para a definição de "empresa" reflete essa evolução, com o Código Civil de 2002 estabelecendo um regime jurídico dedicado às atividades empresariais, reconhecendo as diferenças entre as atividades profissionais e as atividades empresariais.

A caracterização da empresa no Direito brasileiro está centrada em quatro elementos essenciais: o objeto (produção, circulação de bens ou prestação de serviços), a finalidade (intuito lucrativo), a forma (organização dos fatores de produção), e o risco (a assunção de obrigações patrimoniais pelo empresário). A empresa não é apenas um conceito econômico, mas também um constructo jurídico que regula as relações entre os diversos agentes envolvidos na produção e distribuição de bens e serviços.

Contudo, a noção de empresa, embora inicialmente originária da Economia, foi progressivamente incorporada ao Direito, com a legislação se adaptando à complexidade dos fenômenos econômicos. No Brasil, o Código Civil de 2002 dedica seu Livro II ao "Direito de Empresa", definindo o regime jurídico privado aplicável às atividades empresariais. O artigo 966 do Código Civil brasileiro consagra, em seu caput, o conceito de empresa como um elemento essencial para distinguir o campo do Direito Privado.

Embora o conceito jurídico de empresa se aproxime da definição econômica, existem diferenças fundamentais. O Direito brasileiro exclui da definição de empresa atividades que envolvem um vínculo personalíssimo entre o prestador de serviços e o tomador, como as profissões intelectuais, científicas, literárias ou artísticas. Tais

atividades, mesmo que organizadas economicamente e com intuito lucrativo, não se enquadram no regime jurídico da empresa, exceto quando deixam de ter caráter personalíssimo e passam a integrar uma estrutura empresarial.

A caracterização da empresa no Direito brasileiro se apoia em quatro elementos essenciais: o objeto (produção, circulação de bens ou prestação de serviços); a finalidade (intuito lucrativo); a forma (organização dos fatores de produção: capital, recursos naturais, trabalho e tecnologia); e o risco (a assunção de obrigações patrimoniais pelo empresário).

O conceito jurídico de empresa no Brasil é claro ao diferenciar entre a pessoa física ou jurídica que exerce a atividade empresarial e a atividade em si. A empresa é a atividade econômica organizada, e o empresário é o titular dessa atividade, seja pessoa física (empresário individual) ou jurídica (sociedade empresária). A definição jurídica de empresa, portanto, está centrada na organização e exercício de uma atividade econômica com fins lucrativos, não na pessoa do empresário.

Essas distinções jurídicas são fundamentais para a compreensão do papel da empresa no contexto do Direito Privado e para a regulação das relações comerciais e empresariais na sociedade contemporânea.

A evolução da empresa no Direito, desde a regulamentação das atividades comerciais até a incorporação das práticas jurídicas modernas, que envolvem a criação de normas específicas para lidar com as complexidades do mercado. A transformação do conceito de "empresa" no Direito brasileiro refletiu as mudanças da economia, reconhecendo a importância dos contratos e da organização dos fatores de produção no funcionamento das empresas.

A regulamentação jurídica da empresa é um ponto crucial para entender o papel dos *data brokers* no mercado. Com o uso crescente de dados pessoais, é essencial que o Direito estabeleça limites claros para a comercialização desses dados e proteja os direitos dos indivíduos. Assim, a definição jurídica da empresa serve como base para o entendimento das obrigações legais das empresas que lidam com dados pessoais, particularmente no que tange à privacidade e à proteção de dados.

5.3 Direito, Empresa e Eficiência

Sob a ótica econômica, a empresa pode ser analisada em termos de eficiência, especialmente no que se refere à gestão dos custos de transação e à alocação eficaz

dos recursos. O Teorema de Coase é central para essa análise, pois explica como a distribuição eficiente dos direitos de propriedade pode reduzir os custos de transação, facilitando as relações econômicas e contratuais entre os agentes. Em outras palavras, a legislação deve criar condições que favoreçam a alocação eficiente de recursos, facilitando as transações jurídicas necessárias para o funcionamento eficaz da organização.

O papel do Direito, portanto, é essencial para garantir que as transações jurídicas, as relações contratuais estabelecidas para organizar os fatores de produção, ocorram com o menor custo possível. A eficiência jurídica reside na redução dos custos de transação, promovendo um ambiente no qual as negociações e a formalização de contratos sejam ágeis e eficazes. Isso inclui não apenas a regulamentação dos direitos de propriedade, mas também a criação de mecanismos para garantir que os contratos sejam cumpridos de forma eficiente, evitando disputas legais e garantindo a continuidade das atividades empresariais.

A interação entre empresa, economia e Direito é, portanto, multifacetada. A empresa, como unidade de organização econômica, depende de uma base jurídica sólida que sustente a coordenação dos fatores de produção e viabilize as transações necessárias para sua operação. O Direito, ao regular a empresa, não apenas assegura os direitos dos diversos agentes (empresários, trabalhadores, fornecedores, consumidores), mas também influencia diretamente os custos envolvidos nas transações, impactando a eficiência geral do sistema produtivo.

Ao regular os contratos empresariais, a legislação não deve se limitar à sua constituição e funcionamento, mas também buscar estabelecer mecanismos eficientes para a aquisição, manutenção, proteção e transferência de direitos entre os agentes econômicos, com o objetivo de minimizar os custos de transação. O papel ideal da legislação, segundo o que pode ser chamado de Teorema Normativo de Coase, é “estruturar a lei de forma a remover os obstáculos aos acordos privados”. O papel da lei é, portanto, tornar as negociações mais ágeis e facilitar as trocas privadas, de modo que as partes possam ajustar seus direitos de forma eficiente sem a intervenção direta do legislador.

Dessa forma, a disciplina jurídica empresarial deve minimizar os custos enfrentados pelos empresários na celebração de contratos com fornecedores, trabalhadores e financiadores, mediante regras claras, previsíveis e ágeis. A

legislação trabalhista, civil e empresarial, ao disciplinar as relações jurídicas dinâmicas da empresa, assume papel fundamental na coordenação econômica moderna.

a) Aplicação do Teorema no Mercado de Dados:

Essa análise ganha uma nova dimensão no contexto da economia digital. A comercialização direta ou indireta de dados pessoais se tornou um aspecto central da atividade empresarial contemporânea, exigindo a formalização de transações complexas entre titulares de dados, intermediários (data brokers) e empresas interessadas em seu uso. Nesse ambiente, o Teorema de Coase oferece uma lente valiosa para compreender os desafios e limitações da eficiência jurídica e econômica.

Exemplo 1: Data Brokers e Empresas Compradoras de Dados

Imagine que uma empresa deseje adquirir dados de consumidores para personalizar campanhas de marketing. Os *data brokers* atuam como intermediários, reunindo informações de diversas fontes (como redes sociais, históricos de compras e dispositivos móveis) e vendendo esses dados para empresas. Neste cenário:

Propriedade dos dados: Os consumidores ou empresas que geram os dados são, em tese, os titulares desses direitos. Porém, em muitos casos, plataformas digitais e aplicativos assumem o controle sobre os dados mediante cláusulas contratuais, muitas vezes pouco claras.

Custos de transação: O Teorema de Coase afirma que, com custos de transação baixos, os agentes poderiam negociar diretamente sobre o uso, acesso e valor dos dados. Os brokers funcionam como facilitadores dessas transações, reduzindo custos de busca e negociação. Nesse modelo ideal, a transação seria eficiente, beneficiando tanto consumidores (por meio de remuneração ou benefícios) quanto empresas (com dados úteis para suas estratégias).

Exemplo 2: Proteção de Dados Pessoais e Regulação

Com a entrada em vigor de legislações como a LGPD (Lei Geral de Proteção de Dados no Brasil) e a GDPR (Regulamento Geral de Proteção de Dados da União Europeia), o cenário se torna mais complexo.

Propriedade dos dados: A legislação passa a reconhecer explicitamente que os dados pessoais pertencem ao indivíduo, exigindo consentimento claro e informado para qualquer tipo de tratamento.

Custos de transação: A conformidade com essas normas impõe custos jurídicos elevados, obrigações de transparência, políticas de privacidade robustas, auditorias, registros e mecanismos de consentimento. Tais exigências aumentam os custos de transação, tornando a negociação direta mais onerosa e complexa.

b) O Papel dos Data Brokers à Luz do Teorema de Coase:

Na teoria de Coase, os data brokers seriam intermediários eficientes caso operassem em um ambiente de baixa fricção regulatória e alta clareza contratual. Contudo, na prática, atuam em um mercado caracterizado por assimetria de informação, ausência de consentimento efetivo dos titulares dos dados e constantes mudanças no aparato regulatório.

Esses fatores elevam os custos de transação, reduzindo a eficiência das negociações privadas. Por isso, o papel do Direito torna-se ainda mais relevante: proteger os titulares dos dados, garantir transparência, e criar um ambiente institucional que promova equilíbrio entre eficiência econômica e proteção de direitos fundamentais.

c) Limitações e Desafios à Eficiência no Mercado de Dados:

O Teorema de Coase pressupõe que os custos de transação sejam baixos, algo difícil de alcançar no ambiente real do mercado de dados, por diversas razões:

Custos jurídicos elevados: A conformidade com as normas de proteção de dados exige recursos especializados e processos internos complexos.

Assimetria de informação: Consumidores raramente compreendem o real alcance do uso de seus dados, o que inviabiliza uma negociação direta consciente e equilibrada.

Falta de transparência e consentimento eficaz: Muitas vezes, o consentimento é obtido de forma implícita ou através de termos de uso pouco acessíveis, o que compromete a legitimidade da transação.

Intervenção estatal: A regulação surge como resposta à falha de mercado causada por altos custos de transação e desigualdade informacional. A LGPD e a GDPR tentam restaurar o equilíbrio, mesmo que isso represente um aumento dos custos para os agentes econômicos.

O Teorema de Coase fornece um arcabouço teórico importante para compreender a eficiência econômica das relações contratuais dentro das empresas e, especialmente, no contexto do mercado de dados. A ideia de que, com direitos de propriedade bem definidos e custos de transação baixos, as partes podem alcançar uma alocação eficiente dos recursos, oferece base para o desenvolvimento de um Direito Empresarial voltado à eficiência.

No entanto, o mercado de dados demonstra as limitações práticas dessa teoria: a necessidade de regulação, o papel dos intermediários, a assimetria de informação e os custos elevados de conformidade tornam as transações mais complexas do que o modelo ideal prevê. O desafio do Direito, portanto, é estruturar o ambiente regulatório de forma a permitir que as trocas privadas sejam possíveis, eficazes e justas, minimizando os custos de transação sem comprometer os direitos fundamentais dos titulares dos dados.

A análise da eficiência jurídica na gestão das transações empresariais e da distribuição de direitos de propriedade revelou como o direito pode minimizar os custos de transação e fomentar a eficiência das atividades econômicas. A redução desses custos facilita a organização empresarial e a realização de negociações contratuais, o que é essencial para o bom funcionamento do mercado.

Portanto, a eficiência jurídica discutida aqui é particularmente relevante para o mercado de dados pessoais, onde a comercialização desses dados depende de transações contratuais e da implementação de regulamentações eficazes. O papel do Direito, portanto, não é apenas regular a comercialização, mas também garantir que as transações envolvendo dados pessoais sejam realizadas com um mínimo de custos e de forma ética, protegendo os direitos dos consumidores e promovendo uma competição saudável no mercado.

5.4 Estrutura da Empresa na Era Digital

A digitalização tem redefinido de maneira profunda a forma como as empresas operam, impulsionando uma transição para novos modelos de negócios interconectados, mais rápidos e baseados em dados. A conectividade e a velocidade de interação têm sido, de fato, os pilares de uma nova era empresarial, em que a tecnologia desempenha um papel essencial não apenas na produção, mas também na transformação do consumo e das relações de mercado. O conceito de "economia digital" já está consolidado, com a tecnologia como principal motor da criação de riqueza. Como destaca Fabiola Grimaldi (2020), a nova dinâmica empresarial é sustentada por um sistema interligado e eletrônico, que se caracteriza como uma rede global de comunicação e comércio, com a Internet como sua espinha dorsal.

Esse novo cenário impulsionou o surgimento das chamadas empresas digitais, que se caracterizam pela utilização intensiva da internet e das tecnologias digitais em seus modelos de operação. Como argumenta Pinheiro (2019), não se trata apenas de uma mudança na infraestrutura ou no meio de transações, mas de uma transformação mais profunda na própria natureza do consumo, que passa a ser mediado pela coleta e processamento de dados pessoais.

A sociedade digital já assumiu o comércio eletrônico como um novo formato de negócio. Ou seja, não é só o meio que está mudando, mas a própria forma de consumo de produtos. (PINHEIRO. 2019, p.147).

As empresas digitais são definidas como aquelas que usam da tecnologia e principalmente da internet, meio digital, para desenvolver a sua atividade comercial, em uma nova era de mercado, determinada por consumidores cada vez mais conectados (GRIMALDI, 2020, p.120).

Na era da economia digital, os dados pessoais emergem como a principal matéria-prima para a criação de valor. A transformação das informações pessoais em ativos comerciais e o uso desses dados para promover a personalização e otimização de serviços são as principais forças que impulsionam as empresas digitais. Em outras palavras, a utilização estratégica desses dados permite não só a criação de novos produtos e serviços, mas também a aprimoração contínua de ofertas e experiências para os consumidores, como explica Bioni (2019). "Aumentam-se as possibilidades de êxito junto à audiência, seja melhorando a concepção e a segmentação de um produto ou serviço, seja no que pertine à abordagem publicitária para promovê-los." (BIONI. 2019, p.12).

A evolução dessa economia de dados traz consigo novas implicações jurídicas e sociais, particularmente no que se refere à privacidade e à proteção dos dados pessoais. A crescente preocupação com o uso indiscriminado e o compartilhamento de informações pessoais exige uma reflexão sobre os limites éticos e legais que devem ser impostos às empresas. Nesse sentido, a criação de um "direito à privacidade da informação" se torna essencial, como um novo componente dos direitos fundamentais na era digital, o que, segundo Grimaldi (2020), estabelece as bases para a cidadania eletrônica.

A proteção dos dados pessoais é uma evolução da soma de um conjunto de direitos que vem a fundamentar um novo direito fundamental para uma nova cidadania, a cidadania eletrônica ou corpo eletrônico (GRIMALDI, 2020).

A privacidade, que antes era um conceito mais restrito, passa a englobar o direito de proteção de dados pessoais e a preservação da autonomia dos cidadãos em um ambiente digital cada vez mais interconectado. A manipulação e comercialização de dados pessoais por empresas digitais não apenas transformam o mercado de consumo, mas também alteram profundamente as relações sociais e econômicas. Como apontado por Bioni (2019), a informação sobre os hábitos de consumo dos indivíduos cria novas oportunidades de negócios, mas também representa um risco à privacidade e à liberdade do consumidor. “E, nesse sentido, as informações sobre os hábitos de consumo dos cidadãos, afora outros dados pessoais, permitem empreender de forma mais eficiente no mercado.” (BIONI, 2019, p. 12).

Esse contexto de economia digital está intrinsecamente relacionado à Quarta Revolução Industrial, que, conforme Eduardo Goulart Pimenta (2022), é marcada pela convergência de tecnologias como inteligência artificial, computação em nuvem, blockchain e big data. A introdução dessas tecnologias disruptivas tem um impacto direto não só nos processos produtivos, mas também nas formas de distribuição e consumo de bens e serviços. A Indústria 4.0 reflete uma transformação que vai além da automação, envolvendo a digitalização de processos, a interconectividade e a personalização de ofertas para os consumidores.

A utilização estratégica dos dados pessoais e a adaptação das empresas a esse novo modelo de mercado requerem uma série de ajustes estruturais. A criação de novos cargos como o Chief Data Officer (CDO), que supervisiona a governança

dos dados e garante a conformidade com regulamentações como a LGPD (Lei Geral de Proteção de Dados), é um exemplo de como as empresas estão se reorganizando para enfrentar os desafios dessa nova realidade. Além disso, a integração de tecnologias como a Internet das Coisas (IoT) e o big data permite às empresas otimizar não apenas a coleta de dados, mas também o desenvolvimento de produtos e serviços mais eficientes e personalizados.

No entanto, essa transformação digital não é apenas uma mudança tecnológica, mas também uma adaptação cultural e organizacional que afeta todos os níveis das empresas. As empresas precisam ir além da implementação de novas tecnologias; elas devem integrar a ética, a transparência e a responsabilidade no uso de dados como pilares centrais de suas operações. Isso implica não só no cumprimento das regulamentações, mas também no investimento em segurança cibernética e na criação de uma cultura organizacional que respeite os direitos dos consumidores.

Para enfrentar os desafios da era digital, as empresas devem se adaptar de maneira ágil às mudanças do mercado, mas sempre com uma postura ética e transparente em relação ao uso dos dados. Isso envolve a criação de processos internos que garantam a proteção da privacidade dos consumidores e a implementação de práticas robustas de segurança cibernética, como a criptografia e a proteção contra vazamentos de dados. Além disso, a educação contínua sobre privacidade e segurança deve ser parte integrante da formação de todos os funcionários, desde a alta gestão até os colaboradores operacionais, para garantir que todos compreendam a importância do uso ético e responsável dos dados.

A transformação digital também exige uma colaboração mais estreita entre as áreas de marketing, TI e compliance, criando uma abordagem holística que permita que a inovação e a proteção de dados coexistam de forma equilibrada. A inovação, quando guiada por princípios éticos e regulatórios claros, pode trazer benefícios significativos tanto para as empresas quanto para os consumidores, ao mesmo tempo em que preserva a confiança e respeita os direitos dos indivíduos.

Nesse sentido, a estrutura empresarial na era digital está sendo reformulada para incorporar tecnologias emergentes como inteligência artificial, big data e IoT. Esses avanços não apenas aumentam a competitividade e a inovação, mas também exigem uma mudança significativa nas práticas organizacionais, com ênfase na

governança de dados, conformidade regulatória e ética no uso das informações pessoais. Para prosperar nesse novo cenário, as empresas precisam adotar uma abordagem centrada no consumidor, que respeite os direitos fundamentais à privacidade e à segurança, ao mesmo tempo em que aproveita o potencial dos dados para inovar e criar valor.

Por fim, a transformação digital foi explorada como um fator disruptivo que reconfigura os modelos de negócios tradicionais, introduzindo novos desafios e oportunidades. A digitalização e o uso intensivo de dados pessoais tornam as empresas mais ágeis e eficientes, mas também impõem novas exigências no que diz respeito à proteção da privacidade e à conformidade regulatória.

A digitalização e a transformação da estrutura empresarial são diretamente ligadas ao tema da dissertação, pois envolvem a coleta, análise e comercialização de dados pessoais como parte fundamental da estratégia empresarial. O uso de dados na era digital traz à tona questões regulatórias e de privacidade, especialmente com o papel crescente dos *data brokers* na coleta e venda desses dados. O desafio regulatório que as empresas enfrentam na era digital é garantir que sua coleta de dados seja feita de maneira ética e conforme as legislações de proteção de dados, como a LGPD, sem prejudicar a confiança do consumidor, atrelando-se às suas legítimas expectativas.

5.5 O Valor Econômico dos Dados Pessoais: Ativos, Oportunidades e Riscos

Na era digital, os dados pessoais emergem como ativos essenciais para o crescimento das empresas. Sua importância vai além da simples coleta de informações; os dados tornaram-se cruciais para a criação de valor, proporcionando uma vantagem competitiva ao permitir que as empresas personalizem produtos, serviços e campanhas de marketing de forma mais eficiente. A coleta e análise de dados oferece oportunidades excepcionais para otimizar a experiência do cliente, aprimorar a tomada de decisões e gerar novos fluxos de receita.

No entanto, essa transformação também apresenta riscos substanciais, especialmente no que tange à privacidade e segurança. Empresas que não gerenciam adequadamente os dados pessoais podem sofrer danos à sua reputação, multas pesadas e perda de confiança por parte dos consumidores. Em contrapartida, o uso

ético e transparente dos dados permite que as empresas aprimorem sua competitividade e criem relações mais fortes e duradouras com seus clientes.

Assim, o valor econômico dos dados pessoais está diretamente relacionado ao modo como são tratados. Quando explorados corretamente, esses dados podem gerar crescimento sustentável e inovação contínua, refletindo seu papel vital nas estratégias empresariais e modelando o futuro do mercado digital.

Ao analisar o impacto econômico dos dados, fica evidente como eles não apenas influenciam as decisões corporativas, mas também geram oportunidades para novos modelos de negócios. A coleta e o uso inteligente dessas informações proporcionam uma vantagem competitiva, permitindo a personalização de produtos, serviços e campanhas, e otimizando a experiência do consumidor.

Diante desse cenário, é fundamental compreender que os dados pessoais se tornaram ativos essenciais para a inovação e a competitividade das empresas. Sua coleta e análise oferecem não apenas vantagens no aprimoramento da experiência do cliente, mas também abrem portas para novos fluxos de receita e modelos de negócios inovadores. Contudo, o uso inadequado desses dados pode acarretar riscos significativos, como danos à reputação da empresa e possíveis sanções regulatórias. Assim, torna-se imprescindível que as organizações adotem uma abordagem ética e transparente no manejo dos dados, visando manter uma relação de confiança duradoura com seus consumidores.

Nesse contexto, o valor econômico dos dados pessoais ganha ainda mais relevância, especialmente no que diz respeito aos *data brokers*, que desempenham um papel central na coleta, processamento e comercialização dessas informações para outras empresas. A forma como esses dados são tratados e utilizados impacta diretamente as estratégias empresariais, evidenciando a necessidade de um equilíbrio entre inovação e a proteção da privacidade dos indivíduos. O crescimento sustentável das empresas no mercado digital depende, portanto, de uma abordagem ética e regulada, que garanta a conformidade com as normas de proteção de dados e preserve a confiança dos consumidores.

5.6 Inovação, Competitividade e os Riscos da Dependência de Dados Pessoais

O papel dos *data brokers* no mercado de dados pessoais é crucial, pois eles atuam como facilitadores que conectam consumidores e empresas, mediando a

compra e venda de informações. Esses agentes têm o poder de moldar o mercado, pois são responsáveis pela coleta, processamento e comercialização dos dados pessoais dos consumidores. Ao fornecer dados detalhados sobre comportamentos, preferências e interesses dos indivíduos, os *data brokers* permitem que empresas, como os *Content Service Providers (CSPs)*, adotem estratégias de marketing e personalização mais eficazes. Isso pode resultar em campanhas publicitárias mais direcionadas, produtos mais alinhados às necessidades dos consumidores e, conseqüentemente, maior rentabilidade.

Entretanto, a atuação desses intermediários levanta questões sobre a justiça e a transparência no uso dos dados. Os consumidores raramente recebem compensações pelos dados que geram, o que gerou debates sobre a equidade e a ética desse modelo de negócios. A atuação dos *data brokers* não apenas impacta as empresas diretamente, mas também influencia a forma como os consumidores percebem o valor de seus dados pessoais, exigindo uma regulação mais eficaz para equilibrar os interesses das partes envolvidas.

A relação entre inovação e o uso de dados no contexto empresarial é fundamental para impulsionar o crescimento e a competitividade. Empresas que utilizam dados de forma estratégica podem criar novos produtos e serviços, explorar nichos de mercado e aprimorar sua oferta de forma contínua. Casos de sucesso, como o uso de dados para personalização de anúncios, otimização de processos logísticos e desenvolvimento de novos produtos, mostram como a inovação baseada em dados pode transformar o mercado.

O debate sobre os limites da economia de dados frequentemente apresenta um falso dilema: a ideia de que a inovação tecnológica só seria possível à custa da privacidade individual. Modelos de negócios baseados na coleta massiva de dados são defendidos sob a premissa de que oferecem benefícios econômicos e sociais. No entanto, como alerta Zuboff (2018), permitir que a tecnologia evolua sem restrições pode resultar na consolidação de uma sociedade de controle, onde a manipulação comportamental e a vigilância massiva comprometem a liberdade e a autonomia individual.

Embora os dados pessoais representem um recurso valioso para as empresas, a dependência excessiva deles apresenta riscos significativos. Em um primeiro momento, a coleta e análise intensivas de dados podem gerar lucros substanciais,

mas também expõem as organizações a ameaças jurídicas, reputacionais e financeiras. Com a promulgação de regulamentações como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, torna-se imperativo que as empresas ajustem constantemente suas práticas de coleta, processamento e compartilhamento de dados para atender aos padrões legais e éticos.

Além disso, a exploração irresponsável de dados pode minar a confiança dos consumidores. Estudos mostram que os usuários estão cada vez mais atentos à forma como suas informações pessoais são tratadas. Nesse sentido, o respeito à privacidade deixou de ser apenas uma obrigação legal para se tornar um diferencial estratégico. Empresas que adotam práticas transparentes e responsáveis podem fortalecer a fidelidade dos clientes e, ao mesmo tempo, reduzir os riscos associados à falta de conformidade.

Modelos de negócios sustentáveis no contexto dos dados pessoais exigem um equilíbrio entre o uso estratégico das informações para inovação e lucratividade e a garantia da privacidade e segurança dos consumidores. A implementação de mecanismos robustos, como o consentimento explícito, o direito ao esquecimento e a anonimização de dados, é fundamental não apenas para evitar penalidades regulatórias, mas também para construir uma relação sólida e de confiança com os clientes. Esses elementos são essenciais para promover uma economia de dados mais ética, transparente e sustentável.

Nesse sentido, a atuação dos *data brokers* no mercado de dados pessoais, ao conectar consumidores e empresas, tem o potencial de impulsionar a inovação e personalização de produtos e serviços. No entanto, sua presença levanta questões éticas e de justiça no uso desses dados. A dependência excessiva de informações pessoais, se não for gerida com responsabilidade, pode comprometer a confiança do consumidor e expor as empresas a riscos legais e reputacionais. A regulação adequada é, portanto, indispensável para garantir um equilíbrio entre as oportunidades de inovação e a proteção da privacidade individual.

Os *data brokers* são peças centrais na comercialização de dados pessoais e no debate sobre os desafios regulatórios. A inovação e a competitividade impulsionadas pelos dados precisam ser acompanhadas por uma reflexão crítica sobre os riscos da dependência excessiva desses recursos. O tema desta dissertação

destaca a importância da regulamentação, enfatizando como ela pode criar um equilíbrio entre os interesses empresariais e os direitos dos consumidores, promovendo um ambiente de negócios mais ético e justo.

5.7 Implicações Regulatórias no Mercado de Dados: Inovação, Competitividade e Modelos de Negócio

A regulação do uso de dados pessoais desempenha um papel fundamental no equilíbrio entre inovação tecnológica e a proteção de direitos fundamentais. Leis como a LGPD e o GDPR impõem restrições importantes, mas também oferecem oportunidades para empresas que buscam se adaptar a um novo ambiente de conformidade. Longe de serem apenas obstáculos, essas regulamentações podem servir como ferramentas para construir confiança no mercado, reforçar a transparência e fomentar a inovação responsável.

As implicações econômicas das regulamentações são amplas, afetando diretamente as estratégias empresariais. Empresas que implementam práticas eficazes de governança de dados não apenas evitam sanções legais e danos reputacionais, mas também podem se posicionar como líderes em ética digital. Nesse cenário, a conformidade deixa de ser apenas uma obrigação para se tornar uma vantagem competitiva, permitindo que as organizações se destaquem em um mercado cada vez mais exigente.

Além disso, o cumprimento das regulamentações pode estimular o desenvolvimento de soluções tecnológicas inovadoras que conciliem privacidade e desempenho. A criação de ferramentas que priorizem a segurança dos dados, como sistemas de inteligência artificial explicável (*explainable AI*) e tecnologias de preservação de privacidade (*privacy-preserving technologies*), pode representar uma nova fronteira de negócios. Tais inovações não apenas atendem às demandas legais, mas também ajudam a atender às expectativas crescentes dos consumidores por mais controle sobre suas informações pessoais.

Portanto, a regulação oferece às empresas uma oportunidade para revisar seus modelos de negócio e adotar práticas mais alinhadas aos valores de sustentabilidade e ética. A adaptação a esse novo paradigma não deve ser vista como um custo, mas como um investimento estratégico que pode gerar benefícios a longo prazo, consolidando um ambiente competitivo mais justo e resiliente.

A conformidade com as regulamentações, como a LGPD e o GDPR, não deve ser vista apenas como uma obrigação legal, mas como uma vantagem competitiva que permite às empresas promoverem uma economia de dados mais ética e sustentável. A regulação também atua como um mecanismo de controle, que pode equilibrar os interesses das empresas com a necessidade de proteger os dados pessoais dos consumidores, estando intimamente ligada aos desafios que os *Data brokers* enfrentam no mercado digital.

5.7.1 O Modelo de Tarifa de Duas Partes e Seu Impacto no Excedente do Consumidor e no Setor Empresarial

O modelo de tarifa de duas partes é discutido na economia digital, especialmente em mercados baseados em dados, como os que envolvem *Personal Data brokers* (PDBs). Esses intermediários atuam como facilitadores entre consumidores e provedores de serviços e conteúdo (CSPs), influenciando tanto a qualidade do serviço quanto o bem-estar do consumidor. O estudo de Krämer, Schnurr e Haberer (2020) explora os impactos econômicos dos PDBs e questiona se os consumidores realmente se beneficiam da comercialização de seus dados.

a) Modelo de Tarifa de Duas Partes Como Estratégia

O modelo de tarifa de duas partes é uma estratégia comum nos mercados digitais, particularmente aqueles baseados em dados. Nele, os consumidores pagam uma tarifa fixa para acessar um serviço, enquanto os dados gerados durante o uso desse serviço são comercializados, resultando em uma tarifa variável frequentemente não explícita. Segundo Krämer, Schnurr e Haberer (2020), esse modelo pode reduzir o excedente do consumidor – o benefício líquido que ele obtém ao utilizar um serviço. Embora a coleta de dados possa, em algumas situações, melhorar a qualidade do serviço, o processo de apropriação de valor pelos PDBs pode prejudicar esse benefício, pois as empresas podem priorizar a coleta de dados em vez de focar na qualidade do serviço.

Esse modelo descreve como as empresas monetizam a interação com os consumidores por meio da coleta e uso dos dados pessoais gerados durante a prestação de serviços digitais. Ele é composto por dois componentes principais:

- Tarifa fixa: Um valor cobrado ao consumidor para acessar o serviço, geralmente relacionado à qualidade do serviço oferecido.
- Tarifa variável: Uma cobrança indireta baseada na coleta e comercialização dos dados gerados durante o uso do serviço.

b) Impacto da Teoria das Duas Tarifas no Excedente do Consumidor

O impacto do modelo de tarifa de duas partes no excedente do consumidor é significativo. Krämer, Schnurr e Haberer (2020) sugerem que a implementação do modelo de tarifas de duas partes impacta significativamente o excedente do consumidor – o benefício líquido obtido ao utilizar o serviço. Embora a coleta de dados possa melhorar a qualidade do serviço em alguns casos, ela também pode levar à apropriação do valor. Krämer, Schnurr e Haberer (2020) sugerem que o modelo de tarifa de duas partes impacta diretamente o excedente do consumidor, pois a coleta de dados, embora possa melhorar alguns aspectos do serviço, também leva à apropriação de parte do valor gerado, prejudicando o excedente do consumidor.

Quando os PDBs comercializam os dados dos consumidores, o valor gerado por esses dados pode ser capturado por terceiros, em vez de ser plenamente refletido em melhorias diretas para o consumidor. Isso reduz o excedente do consumidor, pois a maximização do valor obtido com os dados pode ocorrer à custa da qualidade do serviço, um fenômeno denominado "apropriação do valor".

Esse processo pode resultar em empresas que, ao invés de investir na melhoria contínua dos seus serviços, se concentram na coleta de dados para gerar receitas adicionais, prejudicando assim o bem-estar do consumidor. Como consequência, os consumidores podem enfrentar a redução na qualidade dos serviços oferecidos ou serem forçados a pagar diretamente por melhorias, criando um dilema: aceitar uma qualidade de serviço inferior ou pagar mais por uma experiência aprimorada.

c) Implicações para as Empresas no Mercado de Dados

Para as empresas, o modelo de tarifa de duas partes, aliado à atuação dos PDBs, impõe desafios significativos. A coleta e monetização dos dados tornam-se essenciais para a geração de receita, o que aumenta a competição entre as empresas que dependem de dados para otimizar suas operações e oferecer produtos mais personalizados. A presença de PDBs, como intermediários que coletam, processam

e comercializam dados pessoais, pode alterar a dinâmica competitiva, forçando as empresas a se adaptarem.

Contudo, conforme observam Krämer, Schnurr e Haberer (2020), a ineficiência na coleta e no processamento de dados pode prejudicar tanto as empresas quanto os consumidores. PDBs ineficientes podem gerar uma redução na qualidade dos serviços digitais, aumentando a pressão competitiva sobre as empresas para maximizar a coleta de dados, sem necessariamente gerar valor agregado. Esse cenário pode levar as empresas a reconsiderar suas estratégias de monetização, equilibrando a coleta de dados com a manutenção da qualidade dos serviços prestados.

Caso os PDBs continuem a capturar grandes porções das receitas derivadas da comercialização dos dados, os CSPs podem ser forçados a explorar novas formas de monetizar os dados, como programas de fidelidade ou ofertas premium, que combinem um valor tangível para os consumidores com a geração de receitas para as empresas.

d) Desafios e Oportunidades para as Empresas

As empresas enfrentam o desafio de se adaptar a esse novo cenário competitivo, especialmente aquelas que dependem fortemente de dados para seus modelos de negócios. A presença de PDBs cria novas dinâmicas competitivas, pressionando as empresas a:

- Melhorar a eficiência no uso de dados para justificar os preços cobrados e a qualidade dos serviços oferecidos.
- Investir em proteção de dados e conformidade com regulamentações, como a LGPD no Brasil, que impactam diretamente como os dados podem ser coletados, processados e monetizados.
- Explorar novas formas de monetização dos dados, como programas de fidelidade ou ofertas premium, que equilibram o uso de dados pessoais com benefícios claros para os consumidores.

As empresas precisam adaptar-se rapidamente a esse novo cenário competitivo, que exige não apenas uma coleta eficiente de dados, mas também a conformidade com regulamentações como a LGPD. O desafio é equilibrar a coleta de dados com a manutenção da qualidade dos serviços, sem prejudicar a experiência do

consumidor. Investir em transparência e segurança pode não apenas mitigar riscos, mas também representar uma vantagem competitiva.

e) Regulação e Eficácia dos PDBs

A eficácia dos PDBs também está intimamente ligada à regulação governamental. As políticas públicas, como o direito à portabilidade de dados e a opção de "Não Vender Meus Dados", têm um papel essencial em mitigar os impactos negativos da atuação dos PDBs. Entretanto, como discutido por Krämer et al. (2020), mesmo com políticas regulatórias eficazes, os consumidores podem ser prejudicados se os PDBs não forem suficientemente eficientes. O mercado de dados pessoais, portanto, exige uma regulação que não apenas proteja os dados dos consumidores, mas também fomente a eficiência na coleta e comercialização desses dados.

O modelo de tarifas de duas partes oferece uma estrutura útil para entender as interações entre PDBs, CSPs e consumidores nos mercados digitais. As empresas que operam nesses mercados devem considerar cuidadosamente como a coleta e monetização de dados afetam não apenas seus resultados financeiros, mas também a experiência do consumidor e a qualidade dos serviços oferecidos.

O desafio está em encontrar o equilíbrio entre maximização da receita e manutenção da confiança e satisfação do consumidor, especialmente em um ambiente onde a concorrência por dados é intensa e as regulamentações de proteção de dados estão se tornando cada vez mais rigorosas.

A regulação deve garantir que as práticas dos PDBs sejam transparentes e justas, criando um equilíbrio entre as necessidades de monetização das empresas e os direitos dos consumidores. O modelo de tarifa de duas partes oferece uma estrutura que permite a análise das interações entre PDBs, CSPs e consumidores, mas sua eficácia depende de como os dados são coletados e utilizados de maneira ética e eficiente.

O modelo de tarifa de duas partes, em que os consumidores pagam uma tarifa fixa para acessar serviços digitais, enquanto seus dados são comercializados de forma indireta, tem implicações econômicas complexas. Este modelo pode reduzir o excedente do consumidor, pois a coleta massiva de dados muitas vezes resulta em serviços de menor qualidade. A exploração dos dados pessoais, apesar de gerar lucro

para as empresas, pode prejudicar a experiência do usuário, o que exige uma regulação mais robusta e eficaz.

Portanto, o modelo de tarifa de duas partes oferece uma perspectiva sobre como os *Data brokers* e as empresas digitais monetizam os dados pessoais. Essa abordagem evidencia o dilema entre a monetização dos dados e a manutenção da qualidade do serviço, destacando a necessidade de regulamentação para evitar a exploração excessiva dos consumidores. As estratégias empresariais devem, portanto, equilibrar a coleta de dados com a preservação da experiência do consumidor e a conformidade com as regulamentações.

5.7.1.1 Desafios Estratégicos e Concorrenciais Criados pelos PDBs

A atuação dos *Personal Data brokers* altera profundamente a dinâmica competitiva dos mercados digitais. A coleta de dados pelos PDBs pode deslocar o equilíbrio competitivo entre CSPs e reduzir a qualidade dos serviços oferecidos aos consumidores. Por um lado, os PDBs oferecem uma oportunidade para as empresas expandirem suas operações por meio de informações detalhadas sobre os consumidores; por outro, há o risco de que a pressão para capturar e comercializar dados acabe comprometendo a qualidade do serviço prestado. Para as empresas, o desafio é encontrar um equilíbrio entre a monetização dos dados e a manutenção da confiança do consumidor, garantindo que as inovações não resultem em uma perda de qualidade que prejudique a experiência do usuário.

Os desafios competitivos criados pelos *Personal Data brokers* (PDBs) refletem como a coleta e comercialização de dados alteram a dinâmica do mercado digital. A pressão para maximizar a coleta de dados pode resultar em um comprometimento da qualidade dos serviços oferecidos aos consumidores. As empresas, portanto, enfrentam a necessidade de equilibrar a monetização dos dados com a satisfação e confiança do usuário, essencial para sua sustentabilidade no mercado.

Os *Data brokers* não apenas afetam as empresas diretamente, mas também os consumidores, alterando a percepção sobre o valor dos seus dados pessoais. Este capítulo reforça a importância da regulamentação para assegurar que as empresas possam monetizar dados de forma ética e responsável, sem prejudicar a confiança do consumidor ou a qualidade dos serviços.

5.7.1.2 Regulação e Sustentabilidade no Mercado de Dados Pessoais

O mercado de dados pessoais não pode prosperar sem uma regulamentação eficaz que equilibre os interesses das empresas e os direitos dos consumidores. Regulamentos como o GDPR e a LGPD são passos importantes para garantir que os consumidores tenham controle sobre seus dados e possam se beneficiar de sua comercialização. Contudo, a regulação não deve se limitar apenas à proteção, mas também à eficiência dos processos de coleta e comercialização dos dados pelos PDBs. Políticas como o direito à portabilidade e o direito de não vender os dados devem ser fortalecidas para garantir que os consumidores não sejam explorados de maneira desigual. Para as empresas, a conformidade com essas regulamentações não é apenas uma obrigação legal, mas uma oportunidade para fortalecer sua imagem e construir relações mais transparentes e confiáveis com os consumidores.

É inegável a importância de uma regulamentação eficaz que proteja tanto os direitos dos consumidores quanto a competitividade das empresas. Regulamentos como o GDPR e a LGPD devem ir além da proteção, visando também a eficiência na coleta e comercialização dos dados. A conformidade com essas regulamentações representa uma oportunidade para as empresas se posicionarem como líderes em ética digital, o que pode ser um diferencial competitivo no mercado.

A regulação e a sustentabilidade do mercado de dados pessoais são temas centrais para entender como os *Data brokers* devem operar de forma transparente e ética. A dissertação explora como a regulamentação pode equilibrar os interesses empresariais com a proteção dos consumidores, destacando a importância da transparência e da confiança no uso dos dados pessoais.

5.7.1.3 A Dinâmica Econômica dos Dados Pessoais e os Desafios para as Empresas

À medida que a economia digital cresce, as empresas precisam adotar uma abordagem estratégica que reconheça os dados pessoais não apenas como um recurso para maximizar lucros, mas também como um componente essencial para garantir a satisfação e fidelização dos consumidores. Organizações que conseguirem equilibrar a monetização dos dados com práticas éticas e o cumprimento das regulamentações estarão mais bem posicionadas para obter uma vantagem competitiva sustentável. Além disso, ao entenderem os impactos das tarifas de duas

partes, a atuação dos *Personal Data brokers* (PDBs) e o papel da regulação, as empresas poderão inovar de forma responsável, garantindo que todos os envolvidos – consumidores, empresas e intermediários – recebam valor de maneira equilibrada e sustentável.

O modelo de tarifa de duas partes, como destacado por Krämer, Schnurr e Haberer (2020), revela a complexidade das interações entre PDBs, CSPs e consumidores nos mercados digitais. Embora esse modelo ofereça uma estrutura para a monetização dos dados pessoais, ele também impõe desafios consideráveis em termos de equilíbrio entre a maximização da receita e a manutenção da qualidade do serviço. A presença de PDBs, ao capturar uma parte significativa do valor gerado pelos dados dos consumidores, pode prejudicar o excedente do consumidor e alterar a dinâmica competitiva entre as empresas. Por isso, tanto as estratégias empresariais quanto às políticas regulatórias devem ser cuidadosamente formuladas para garantir que todos os participantes do mercado — consumidores, CSPs e PDBs — se beneficiem de maneira equilibrada e sustentável.

As empresas devem lidar com uma série de desafios ao navegar pelo mercado de dados pessoais. A crescente dependência da coleta e análise de dados coloca em risco o equilíbrio entre gerar receita e manter a qualidade do serviço. Para ter sucesso, as empresas precisam:

- a) **Integrar dados de maneira estratégica:** Utilizar dados não apenas para personalizar serviços, mas também para melhorar a experiência geral do consumidor.
- b) **Adaptar-se a regulamentos rigorosos:** Com a implementação de regulamentações como a LGPD e o GDPR, as empresas devem garantir conformidade, ao mesmo tempo em que preservam a confiança do consumidor.
- c) **Explorar novas formas de monetização:** Oferecer soluções inovadoras, como programas de fidelidade ou ofertas premium, que combinem monetização de dados com benefícios tangíveis para os consumidores e com as suas expectativas.

O verdadeiro desafio reside em encontrar um equilíbrio entre a maximização da receita e a preservação da confiança e satisfação do consumidor, especialmente em um cenário de intensa competição por dados e regulamentações cada vez mais rigorosas na proteção da privacidade. A regulação precisa assegurar que as práticas dos *Personal Data brokers* (PDBs) sejam transparentes e justas, criando um ponto de equilíbrio entre as necessidades de monetização das empresas e os direitos dos consumidores. Neste contexto, a transparência e a segurança no tratamento dos dados não são apenas requisitos legais, mas também uma vantagem competitiva crucial.

A eficácia do modelo de tarifa de duas partes está diretamente ligada à forma como os dados são coletados e utilizados de maneira ética e eficiente, garantindo que todos os envolvidos no mercado — consumidores, empresas e intermediários — se beneficiem de maneira justa e sustentável. Esse equilíbrio é essencial para a manutenção de uma economia de dados que respeite os direitos dos consumidores e, ao mesmo tempo, impulsiona a inovação.

Por fim, a dinâmica econômica dos dados pessoais, com foco nos desafios enfrentados pelas empresas e intermediários como os *Data brokers*, revela a complexidade do mercado digital. As regulamentações e as estratégias empresariais devem se adaptar e evoluir constantemente para garantir que os dados pessoais sejam utilizados de forma ética, transparente e sustentável, refletindo a importância de equilibrar inovação e a proteção da privacidade.

6 ESTRATÉGIAS EMPRESARIAIS: EQUILÍBRIO ENTRE INOVAÇÃO E ECONOMIA E MERCADO ÉTICO DE DADOS E A PROTEÇÃO DE DADOS

6.1 *Privacy by Design* no contexto da Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados (LGPD) representa um marco regulatório essencial para o tratamento de dados pessoais no Brasil, estabelecendo diretrizes claras e rigorosas para a privacidade. Ela não se limita apenas a reforçar práticas já presentes nas organizações, mas amplia a visão sobre a segurança da informação, enfatizando a necessidade de incorporar a privacidade desde a fase inicial de qualquer projeto, produto ou serviço. Esse enfoque propõe a *privacy by design* como um princípio vital para o desenvolvimento de empresas, especialmente em estágios

iniciais, exigindo que a privacidade seja considerada de maneira proativa, e não reativa (Grimaldi, 2020).

O conceito de *privacy by design*, criado por Ann Cavoukian na década de 1990, defende que a privacidade deve ser integrada desde a concepção de sistemas e serviços, incorporada de maneira estruturada e permanente, não apenas como uma adição posterior (Cavoukian, 1995). Embora a LGPD não mencione explicitamente o termo "*privacy by design*", ela adota práticas alinhadas a esse conceito.

Para Bioni (2019, p.84), o *Privacy by Design* "é a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção de dados pessoais."

Por exemplo, o artigo 46 da LGPD obriga os agentes de tratamento a implementar medidas de segurança e proteção desde a fase de concepção de produtos ou serviços.

Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

[...]

§ 2º 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. (Brasil, 2018).

Portanto, a LGPD adota uma abordagem proativa para a proteção de dados pessoais, incorporando um conceito essencial de *privacy by design*. No artigo 6º da lei, destacam-se dois princípios fundamentais: segurança e prevenção. A segurança é garantida por meio de medidas técnicas e administrativas adequadas para proteger os dados pessoais contra acessos não autorizados ou contra situações acidentais de destruição. Já a prevenção envolve a adoção de medidas antecipatórias para evitar danos causados pelo tratamento inadequado dos dados (Brasil, 2018).

Outro princípio relevante de *privacy by design* adotado pela LGPD é a proteção ao longo de todo o ciclo de vida dos dados. A lei assegura que a proteção se estenda desde a coleta até a eliminação dos dados pessoais. O artigo 18, inciso IV, garante ao titular dos dados o direito de solicitar a eliminação de dados desnecessários ou tratados de maneira inadequada (Brasil, 2018). Esse princípio se alinha à ideia de que

a privacidade deve ser garantida de forma contínua e abrangente, desde a coleta até o descarte dos dados, e não apenas em momentos específicos de seu tratamento.

A transparência não só fortalece a confiança dos usuários em relação ao uso de seus dados, mas também facilita a responsabilização das empresas em casos de incidentes de segurança (Jimenez, Maldonado & Opice Blum, 2018). A LGPD, assim, não apenas exige a conformidade com a proteção de dados, mas também promove uma mudança cultural nas organizações, incentivando-as a adotar uma cultura de privacidade que permeia todos os níveis de sua operação.

Em síntese, embora o conceito de *privacy by design* não seja explicitamente mencionado na LGPD, a lei reflete os princípios centrais dessa metodologia, exigindo que as empresas integrem práticas de proteção de dados pessoais desde a concepção de seus produtos e serviços. A inclusão da privacidade no design de sistemas vai além de uma obrigação legal; trata-se de uma estratégia essencial para garantir a confiança do consumidor e a segurança dos dados, elementos fundamentais no contexto da economia digital.

Além disso, o conceito de *Privacy by Default* (privacidade como padrão) está diretamente relacionado ao *Privacy by Design*. Uma das maneiras de garantir a privacidade desde o início do desenvolvimento é assegurar que o produto ou serviço, quando lançado ao público, já esteja configurado com todas as medidas de proteção de dados implementadas como padrão.

Sobre essa questão, Pinheiros destaca:

Podemos dizer que o Privacy by Design é uma decorrência do Privacy by Default. Em outras palavras, trata-se da ideia de que o produto ou serviço seja lançado e recebido pelo usuário com todas as salvaguardas que foram concebidas durante o seu desenvolvimento. O princípio da proteção de dados por padrão é reconhecer o mínimo necessário em relação aos dados (às finalidades do tratamento pretendido), proibindo que esses dados excedam tais finalidades. (PINHEIRO, 2018, p.399).

Em outras palavras, quando o produto ou serviço for lançado, as configurações de segurança e proteção de dados devem ser implementadas como padrão. Dessa forma, a coleta de dados só deve ocorrer quando realmente essencial, em conformidade com os princípios de minimização de dados. Adicionalmente, é fundamental proporcionar ao usuário a liberdade de, se preferir, ativar de forma voluntária configurações extras ou funcionalidades voltadas para a privacidade.

6.2 Integrando *Privacy by Design* nas Estratégias Empresariais

Em um ambiente dinâmico e de constante inovação como o das empresas de base tecnológicas, é fundamental que a proteção de dados e a privacidade sejam incorporadas desde a concepção do negócio. A Lei Geral de Proteção de Dados (LGPD) exige que, desde os primeiros passos de um projeto, a segurança e a privacidade sejam parte da estratégia de desenvolvimento, garantindo não apenas o cumprimento das regulamentações brasileiras, mas também oferecendo uma base sólida para a segurança jurídica do negócio no futuro.

O cumprimento das normativas, incluindo a LGPD, é essencial para o sucesso e crescimento das empresas, independentemente de seu estágio de desenvolvimento. Afinal, a responsabilidade empresarial é uma exigência universal, e nenhuma organização, por menor que seja, está isenta de responder por suas ações, mesmo nos primeiros momentos de sua jornada.

A adoção do conceito de *privacy by design* não se limita ao cumprimento da legislação brasileira, mas também se alinha a uma tendência global crescente de proteção de dados. Isso se torna ainda mais relevante, pois a proteção da privacidade dos usuários, empreendedores e investidores contribui diretamente para a construção de um negócio sustentável e viável. Em um mercado altamente competitivo, a adequação aos princípios da LGPD e ao *privacy by design* pode consolidar as bases do crescimento das empresas, diminuindo riscos e aumentando sua credibilidade.

Incorporar os princípios do *privacy by design* exige que a empresa adote uma abordagem holística desde a fase inicial do projeto. Para isso, é necessário garantir que o desenvolvimento do produto, serviço ou ideia esteja alinhado com as melhores práticas de proteção de dados, sem comprometer a funcionalidade e os objetivos do modelo de gestão da empresa. Uma equipe multidisciplinar, engajada e preparada, é crucial para garantir a segurança dos dados pessoais, atendendo a todas as exigências da LGPD, enquanto mantém a eficiência e os propósitos da organização.

Além disso, é importante notar que as normas de proteção à privacidade e dados pessoais não se limitam ao Brasil, mas se configuram como uma tendência global. A falta de conformidade com a LGPD não só prejudica os negócios locais, mas também pode comprometer a expansão global. Assim, adotar o *privacy by design* é uma estratégia que não apenas protege a startup contra falhas no tratamento de

dados e vazamentos, mas também garante sua adequação aos padrões internacionais.

A cada dia, os consumidores estão mais conscientes de seus direitos em relação à privacidade e proteção dos dados pessoais. Estar em conformidade com a LGPD e adotar a postura proativa do *privacy by design* é fundamental para conquistar a confiança do público. Caso contrário, as empresas podem enfrentar resistência à adesão a seus produtos e serviços, o que impacta diretamente seu sucesso no mercado.

Por fim, as empresas que aplicam o conceito de proteção de dados desde o início de sua concepção têm um diferencial competitivo significativo. Garantir a privacidade e segurança das informações de seus usuários não apenas promove a confiança, mas também atrai investidores, consolidando a reputação e a viabilidade do negócio a longo prazo.

6.3 Privacy by Design e Data Brokers

O conceito de *privacy by design* tem um impacto significativo sobre o papel dos intermediários de dados, como os *data brokers*. Esses profissionais, que operam como intermediários no mercado de dados pessoais, comercializam ou compartilham informações sem o consentimento claro dos indivíduos. Em um cenário onde a proteção de dados se tornou um requisito essencial, especialmente à luz da LGPD, as práticas dos *data brokers* precisam ser ajustadas para garantir que estejam em conformidade com as leis de privacidade e para promover o uso ético dos dados pessoais.

Para integrar de maneira eficaz o *privacy by design* no ambiente dos *data brokers*, as empresas devem adotar práticas que assegurem que os dados sejam coletados e processados de forma transparente, ética e segura. Isso envolve a implementação de medidas que garantam a minimização dos dados, a obtenção de consentimento expresso dos titulares, a transparência nas operações e a proteção dos dados contra acessos não autorizados. Além disso, a adoção de políticas claras de transparência e controle, que permitam aos consumidores visualizar, modificar ou excluir seus dados, é fundamental para respeitar os direitos dos indivíduos e promover um mercado de dados ético.

A regulamentação também precisa ser aprimorada para garantir que os dados pessoais não sejam comercializados sem o devido consentimento ou em desacordo com as diretrizes da LGPD. A criação de sistemas de licenciamento e registro obrigatório, transparência nas práticas de coleta e processamento de dados, e a exigência de consentimento expresso são medidas necessárias para garantir que a atividade dos corretores seja conduzida de maneira ética e em conformidade com a legislação.

A responsabilidade solidária entre as empresas que coletam dados e os intermediários que processam essas informações é uma maneira eficaz de assegurar que todos os envolvidos no ciclo de tratamento de dados compartilhem a responsabilidade por sua proteção. Isso inclui a implementação de auditorias independentes e a criação de penalidades rigorosas para o descumprimento das normas, o que desincentivaria práticas inadequadas e ajudaria a promover uma cultura de privacidade e proteção de dados no mercado.

O *Privacy by Design* é uma abordagem que integra a privacidade nas operações de negócios e na concepção de novos produtos ou serviços desde o início. Em vez de ser uma consideração posterior, a privacidade deve ser uma prioridade desde o início de cada processo que envolva dados pessoais. Para que o *Privacy by Design* seja eficaz, ele deve ser implementado em várias camadas dentro das organizações observando os seguintes critérios:

- a) **Minimização de Dados:** As empresas devem coletar apenas os dados necessários para alcançar os objetivos pretendidos. O princípio da minimização de dados está alinhado com o conceito de que menos dados reduzem o risco de violações de privacidade;
- b) **Proteção por Padrão:** A privacidade deve ser configurada como a configuração padrão para todos os produtos e serviços. Ou seja, as opções de privacidade mais fortes devem ser a escolha inicial para os consumidores, e não uma opção que precisa ser ativada;
- c) **Transparência e Controle:** As empresas devem garantir que seus processos de coleta e uso de dados sejam transparentes, oferecendo aos consumidores controle total sobre seus dados, incluindo opções para modificar ou excluir suas informações;

- d) **Segurança Integrada:** A segurança deve ser incorporada desde o início de cada projeto. Isso implica no uso de tecnologias robustas de criptografia e autenticação, para garantir que os dados sejam protegidos contra acessos não autorizados;
- e) **Avaliações de Impacto sobre a Privacidade:** As empresas devem realizar avaliações de impacto sobre a privacidade (PIAs) sempre que um novo processo ou tecnologia for introduzido, avaliando os riscos para a privacidade e segurança dos dados pessoais.

Integrar o *Privacy by Design* não só ajuda a criar produtos mais seguros e respeitosos com os dados dos consumidores, mas também prepara as empresas para cumprir as regulamentações, como o GDPR e a LGPD, que exigem a adoção de medidas para garantir a privacidade desde a concepção de novos sistemas.

Nesse contexto, o equilíbrio entre inovação, economia e proteção de dados pessoais é um desafio contínuo para as empresas, consumidores e reguladores. A adoção de práticas éticas e transparentes, a implementação do *Privacy by Design* e o fortalecimento das regulamentações de dados são passos fundamentais para garantir que a coleta e o uso de dados pessoais sejam feitos de forma responsável, respeitando os direitos dos consumidores e promovendo um mercado ético de dados. Além disso, a educação e a conscientização sobre privacidade devem ser fortalecidas, garantindo que todos, desde os consumidores até os profissionais da área, compreendam a importância da proteção de dados na era digital.

6.4 Diretrizes para a Melhoria das Práticas de Coleta e Uso de Dados Pessoais pelas Empresas

A era digital transformou profundamente os modelos de negócios, com as empresas cada vez mais dependentes da coleta, processamento e análise de grandes volumes de dados. Esses dados, coletados tanto diretamente dos consumidores quanto por meio de intermediários, são fundamentais para a personalização de produtos e serviços, bem como para a tomada de decisões estratégicas. No entanto, o uso crescente de dados pessoais levantou sérias questões sobre privacidade, transparência e segurança. Nesse cenário, o desafio das organizações é equilibrar a

necessidade de inovação e crescimento econômico com o respeito pelos direitos dos consumidores e a proteção de dados pessoais, criando um mercado ético de dados.

A coleta de dados pessoais é uma das questões centrais no tratamento de informações sensíveis. Para que o mercado de dados seja ético e confiável, é imprescindível que as empresas adotem práticas transparentes, responsáveis e seguras. O consentimento informado é um dos pilares fundamentais da proteção de dados, permitindo que os consumidores compreendam e controlem como seus dados são usados (European Union, 2016) bem como exige que as organizações forneçam aos consumidores informações claras e acessíveis sobre o tipo de dados coletados, as finalidades de sua coleta, como serão armazenados e por quanto tempo serão retidos. Além disso, é essencial que as empresas ofereçam aos consumidores a capacidade de alterar, revisar ou revogar seu consentimento a qualquer momento. Essas práticas aumentam a transparência e a confiança, fundamentais para a construção de um mercado ético de dados.

Uma abordagem eficaz para melhorar a transparência e as práticas de consentimento é a adoção do *Privacy by Design* (Privacidade desde a concepção), que garante que a proteção de dados seja incorporada em todas as fases de desenvolvimento de produtos e serviços. O *Privacy by Design* exige que as empresas planejem e implementem a privacidade como uma característica intrínseca desde o início de qualquer processo que envolva dados pessoais. Essa abordagem não deve ser tratada como uma adição posterior, mas como parte central da estratégia organizacional.

Estratégias para garantir o Consentimento Informado e a Transparência:

- a) **Clareza nos Termos de Consentimento:** A linguagem utilizada para obter consentimento deve ser simples, direta e livre de jargões legais ou técnicos. O consumidor deve ter a certeza de que entende exatamente como seus dados serão usados. Um exemplo disso é o uso de painéis de controle acessíveis que informam claramente os tipos de dados coletados e os fins para os quais serão utilizados;
- b) **Gestão Facilitada de Preferências:** As empresas devem criar sistemas que permitam aos consumidores revisar, modificar ou revogar seu consentimento de forma simples e sem fricções. Isso pode incluir o fornecimento de painéis

de controle personalizados e configuráveis, como exemplificado pela política de privacidade da Apple e outras plataformas tecnológicas líderes;

- c) **Auditoria e Relatórios:** As empresas devem realizar auditorias regulares das suas práticas de coleta e uso de dados, gerando relatórios acessíveis aos consumidores e autoridades, garantindo que estão em conformidade com as leis de proteção de dados, como a LGPD e o GDPR. Essas auditorias devem ser independentes e realizadas por entidades externas para garantir a imparcialidade do processo.

6.5 Fortalecimento das Políticas Regulatórias e Mecanismos de Fiscalização

À medida que o uso de dados pessoais se torna cada vez mais central no desenvolvimento de tecnologias avançadas como IA e aprendizado de máquina, é imperativo fortalecer as políticas regulatórias. A regulação deve não apenas assegurar que as empresas cumpram as normas de proteção de dados, mas também proteger os consumidores contra práticas abusivas, especialmente aquelas envolvendo *data brokers*, que frequentemente comercializam dados pessoais sem o consentimento claro dos titulares.

O aprimoramento das regulamentações sobre a proteção de dados pessoais é uma necessidade premente para garantir maior segurança e transparência no uso das informações no ambiente digital. Em particular, deve-se focar na criação de diretrizes mais rigorosas sobre a coleta, processamento e compartilhamento de dados por terceiros, especialmente quando se trata de intermediários de dados, como os *data brokers*. A implementação de regras claras e eficazes para esses operadores é essencial para proporcionar maior controle aos titulares de dados sobre o uso de suas informações pessoais.

Propostas para aprimorar a regulação existente:

- a) **Licenciamento e Registro de *Data brokers*:** A criação de um sistema de licenciamento e registro obrigatório para *data brokers* seria uma medida eficaz para regulamentar a atuação desses intermediários. Eles seriam obrigados a registrar suas atividades junto às autoridades competentes, o que incluiria a obrigatoriedade de reportar publicamente suas práticas de coleta, processamento e venda de dados pessoais. Isso garantiria maior

visibilidade e fiscalização sobre as operações dessas empresas, além de permitir que os consumidores saibam quem está acessando e utilizando seus dados;

- b) **Transparência e Consentimento Expresso:** Para assegurar que os dados pessoais sejam tratados de forma ética e legal, deve-se exigir que todos os intermediários obtenham o consentimento explícito e informado dos titulares de dados antes de realizar qualquer operação envolvendo suas informações pessoais. Além disso, esse consentimento deve ser renovado periodicamente, garantindo que os indivíduos tenham controle contínuo sobre como seus dados são utilizados. A transparência deve ser uma prioridade, e as empresas precisam informar claramente os objetivos e a natureza do tratamento dos dados;
- c) **Responsabilidade Solidária:** A responsabilidade solidária é um mecanismo importante para garantir que todas as partes envolvidas no tratamento de dados pessoais — desde as empresas que coletam as informações até os intermediários que as processam — compartilhem a responsabilidade no caso de violações dos direitos dos consumidores. Isso implica que, em situações de vazamentos de dados ou uso indevido, as empresas que coletam dados não podem se eximir de responsabilidade, mesmo que os dados tenham sido processados ou vendidos a terceiros. A responsabilização conjunta contribuiria para aumentar a responsabilidade e a conscientização das empresas sobre o tratamento adequado dos dados;
- d) **Fiscalização e Auditoria transparente:** Para garantir a eficácia das regulamentações e a conformidade das empresas com as normas de proteção de dados, é fundamental instituir um sistema de fiscalização robusto e auditorias regulares. A implementação de auditorias independentes e a exigência de relatórios periódicos sobre as práticas de tratamento de dados pelos intermediários tornaria possível detectar e corrigir falhas rapidamente. As auditorias devem ser transparentes e acessíveis ao público, permitindo que os consumidores e as autoridades possam acompanhar a conformidade das empresas com a legislação;
- e) **Criação de Penalidades mais rigorosas:** O endurecimento das penalidades para o descumprimento das normas de proteção de dados

peçoais também é uma medida fundamental para assegurar que as empresas tratem as informações com a seriedade que elas demandam. Multas pesadas, suspensão das atividades de coleta de dados e outras sanções devem ser impostas às empresas que não cumprirem os requisitos legais, especialmente em casos de negligência ou danos irreparáveis aos titulares dos dados. A aplicação rigorosa dessas penalidades pode desincentivar práticas inadequadas e promover uma maior adesão à regulação.

6.6 Educação e Conscientização no Uso de Dados

Em um cenário cada vez mais digitalizado e interconectado, a educação e a conscientização sobre a proteção de dados pessoais se tornam elementos imprescindíveis para a criação de um ambiente seguro e ético de utilização dessas informações. A crescente coleta, processamento e análise de dados exigem que tanto os consumidores quanto as empresas compreendam plenamente os riscos envolvidos, adotando práticas que assegurem a privacidade e o respeito aos direitos individuais.

A educação e a conscientização sobre a proteção de dados são essenciais para garantir que tanto consumidores quanto empresas adotem práticas responsáveis. Grande parte dos consumidores não compreende totalmente os riscos associados ao uso e compartilhamento de seus dados pessoais. Assim, iniciativas de conscientização e educação são fundamentais para equipar tanto indivíduos quanto empresas com os conhecimentos necessários para navegar nesse novo cenário.

Para os consumidores, o entendimento sobre os próprios direitos relacionados aos dados pessoais, como o direito ao consentimento informado, à correção, eliminação e portabilidade dos dados, é essencial para que possam tomar decisões mais conscientes em relação ao compartilhamento de suas informações. As campanhas digitais educativas podem desempenhar um papel crucial nesse processo, fornecendo informações claras e acessíveis sobre como proteger a privacidade e evitar abusos no uso de seus dados.

No contexto corporativo, as empresas devem adotar uma abordagem proativa, implementando treinamentos contínuos para todas as equipes, desde os departamentos de TI até as áreas de marketing e atendimento ao cliente. A

conscientização interna não só contribui para a conformidade com as leis de proteção de dados, como a LGPD, mas também fortalece a cultura de responsabilidade e respeito pela privacidade dos usuários. Além disso, ao promover práticas de privacidade e segurança da informação, as empresas não apenas protegem seus clientes, mas também garantem sua credibilidade e competitividade no mercado.

Propostas para Campanhas de Conscientização e Treinamentos Corporativos:

- a) **Campanhas Digitais e Educativas:** Desenvolver campanhas públicas e privadas para educar os consumidores sobre como proteger seus dados pessoais, como lidar com consentimento e os riscos associados ao compartilhamento de informações, em busca de exaurir a transparência;
- b) **Treinamentos Empresariais Regulares:** Estabelecer treinamentos corporativos regulares para funcionários de todos os departamentos sobre privacidade e segurança da informação. Esses treinamentos devem ser obrigatórios e contínuos, englobando todos os níveis hierárquicos dentro das organizações;
- c) **Parcerias com Instituições Educacionais:** Trabalhar com universidades e escolas para incorporar a proteção de dados na grade curricular, preparando uma nova geração de consumidores, empresas e profissionais conscientes. As parcerias com instituições educacionais são outro caminho importante para a formação de uma geração mais consciente sobre os direitos e responsabilidades no que diz respeito à proteção de dados. Incorporar a proteção de dados nas grades curriculares prepara não apenas os futuros consumidores, mas também os profissionais que atuarão no mercado digital, garantindo que compreendam e integrem as boas práticas de privacidade desde a formação acadêmica.

Nesse contexto, ao analisar o impacto dos *data brokers* na comercialização de dados pessoais, torna-se evidente que a educação e a conscientização desempenham um papel fundamental na construção de um mercado de dados mais ético e transparente. Compreender os direitos de privacidade e as implicações do uso

de dados pessoais é essencial para que os consumidores possam tomar decisões informadas e seguras.

Nesse cenário, as empresas que lidam com dados — incluindo os intermediários, como os *data brokers* — têm a responsabilidade de educar seus clientes sobre o uso e o compartilhamento de suas informações. Isso exige uma mudança cultural dentro das organizações, na qual a transparência e o respeito aos direitos dos consumidores não sejam apenas obrigações legais, mas também um diferencial competitivo. A adoção de práticas como o *Privacy by Design*, por exemplo, pode ser fortalecida por campanhas educativas, possibilitando que as empresas construam relações mais confiáveis com seus clientes, ao mesmo tempo em que promovem a conformidade com regulamentações como a Lei Geral de Proteção de Dados (LGPD).

A promoção da educação sobre privacidade e proteção de dados não deve se restringir apenas aos consumidores, mas também envolver as próprias empresas e os intermediários de dados. A conscientização contínua dentro das organizações sobre a importância da proteção dos dados pessoais é crucial para garantir que as práticas de coleta, processamento e comercialização de dados sejam realizadas de maneira ética, responsável e em conformidade com a legislação.

Programas de treinamento internos e parcerias com instituições educacionais, com o objetivo de integrar a proteção de dados desde a formação acadêmica, são iniciativas essenciais para criar uma cultura de privacidade desde cedo. Dessa forma, a implementação eficaz de políticas educacionais e de conscientização se apresenta como um pilar indispensável para o desenvolvimento de um mercado de dados mais seguro, no qual os desafios regulatórios enfrentados pelos *data brokers* sejam minimizados e o uso de dados pessoais seja conduzido com ética e respeito aos direitos dos indivíduos.

Dentro desse contexto, a relevância do mercado ético de dados e da proteção de dados pessoais se torna ainda mais clara, especialmente quando analisamos a Lei Geral de Proteção de Dados (LGPD) e o conceito de *Privacy by Design*. A análise demonstrou que a privacidade não deve ser tratada apenas como uma obrigação legal ou uma preocupação secundária, mas sim como um princípio fundamental, a ser integrado desde a concepção de novos produtos, serviços e modelos de negócios. A LGPD, ao adotar a abordagem do *Privacy by Design*, estabelece um marco regulatório

robusto que assegura a proteção dos dados pessoais, garantindo, ao mesmo tempo, a transparência, segurança e respeito aos direitos dos indivíduos.

Além disso, foi discutido como a aplicação do *Privacy by Design* por empresas de todos os ramos, inclusive, intermediários de dados, como os *data brokers* que desempenham um papel central na coleta, comercialização e compartilhamento de dados pessoais. A incorporação de práticas éticas e transparentes em suas operações, juntamente com a implementação de medidas regulatórias mais rigorosas, é fundamental para garantir um mercado de dados mais responsável e seguro.

O fortalecimento das políticas regulatórias e a implementação de mecanismos eficazes de fiscalização são, sem dúvida, cruciais para assegurar que as empresas cumpram as normas de proteção de dados, protegendo assim os direitos dos consumidores. Nesse contexto, a educação e a conscientização sobre privacidade e segurança de dados emergem como fatores-chave para criar um ambiente digital mais ético e seguro. Campanhas de conscientização, treinamentos regulares e parcerias com instituições educacionais são iniciativas indispensáveis para que tanto consumidores quanto empresas possam compreender os riscos envolvidos e adotar uma postura responsável no tratamento dos dados pessoais.

Portanto, ao priorizar a privacidade e a proteção dos dados desde o início do desenvolvimento de novos produtos e serviços, e ao fortalecer as estratégias de conscientização e regulamentação, as empresas não apenas asseguram a conformidade com a legislação, mas também criam uma base sólida para a confiança do consumidor, a sustentabilidade dos negócios e o fortalecimento de um mercado ético de dados. O equilíbrio entre inovação, privacidade e segurança será, sem dúvida, um dos principais fatores para o sucesso das organizações em um cenário digital em constante transformação.

7 CONCLUSÃO

A transição para uma sociedade orientada por dados, impulsionada pela digitalização, representa uma transformação profunda e irreversível que afeta as esferas tecnológica, social, econômica e jurídica. Esse processo de "datificação", que converte comportamentos e atividades cotidianas em dados digitais, redefine as relações entre indivíduos, empresas e governos. O fenômeno é intensificado pela ascensão dos *data brokers*, intermediários que coletam, processam e comercializam

dados pessoais, com o objetivo de criar perfis detalhados e prever comportamentos, impactando diretamente a privacidade e autonomia dos cidadãos.

A análise empreendida nesta dissertação evidenciou que, embora a atuação dos *data brokers* contribua para o desenvolvimento de soluções inovadoras e modelos de negócio mais eficientes, ela também levanta desafios significativos no tocante à privacidade, à transparência e à autodeterminação informativa. A comercialização indiscriminada de dados pessoais compromete direitos fundamentais e mina a confiança do consumidor, criando um ambiente de incertezas quanto ao uso e à proteção das informações pessoais.

Diante desse cenário, a regulação jurídica surge como mecanismo indispensável para promover equilíbrio entre interesses econômicos e a proteção de direitos fundamentais. Normas como a Lei Geral de Proteção de Dados (LGPD), no Brasil, o *Regulamento Geral de Proteção de Dados* (GDPR), na União Europeia, e a *California Consumer Privacy Act* (CCPA), nos Estados Unidos, representam avanços expressivos na tentativa de impor balizas ao tratamento de dados pessoais. Contudo, tais regulamentações enfrentam desafios práticos, como a dificuldade de fiscalização, a disparidade entre legislações nacionais e a velocidade com que a tecnologia evolui.

Nesse contexto, conclui-se que a simples existência de normas legais não é suficiente. A efetividade da proteção de dados depende da consolidação de uma governança robusta, que envolva fiscalização eficaz, práticas de transparência ativa e o engajamento das empresas na adoção de políticas preventivas. Medidas como o “*Privacy by Design*” e auditorias regulares devem ser incorporadas às práticas corporativas, com vistas a assegurar o uso ético e responsável dos dados. As organizações, ao tratarem os dados como ativos estratégicos, devem também reconhecer sua responsabilidade jurídica e moral, agindo conforme os princípios da finalidade, necessidade, proporcionalidade, transparência e segurança.

A pesquisa evidenciou ainda que a análise das implicações econômicas da comercialização de dados revela a complexidade do cenário atual, em que a coleta de informações se tornou uma das principais fontes de valor para as empresas. Embora a monetização de dados seja uma estratégia amplamente adotada no mercado digital, ela impõe desafios à confiança do consumidor e à manutenção da qualidade dos serviços. O modelo de tarifa de duas partes, frequentemente utilizado, exemplifica como os dados dos consumidores são empregados para maximizar

lucros, o que pode comprometer a confiança nas práticas empresariais. Nesse sentido, a regulação assume papel crucial ao garantir que as empresas atuem de maneira ética, conciliando a proteção dos consumidores com a competitividade no mercado.

A partir da análise da intersecção entre direito, economia e eficiência, ficou evidente que a regulamentação jurídica desempenha papel duplo: proteger os indivíduos e assegurar um ambiente empresarial previsível e competitivo. As transações jurídicas, sejam contratuais ou regulatórias, são instrumentos indispensáveis para criar um ecossistema digital que concilie inovação com responsabilidade. O grande desafio está em compatibilizar os avanços tecnológicos com a garantia da privacidade e da segurança dos dados, promovendo um modelo de desenvolvimento sustentável e humanizado.

A ideia de tratar a privacidade como propriedade, embora atraente sob a ótica da livre disposição patrimonial, demanda cautela. Os dados pessoais, por estarem intrinsecamente ligados à identidade e à dignidade do indivíduo, não podem ser objeto de mercantilização irrestrita. A LGPD, ao não proibir a comercialização, estabelece limites rigorosos baseados no consentimento informado e nos princípios fundamentais que garantem a proteção da personalidade, especialmente a liberdade, a privacidade e a autodeterminação informativa. Assim, a utilização econômica dos dados é juridicamente admissível, desde que respeite tais fundamentos constitucionais e os princípios da finalidade, necessidade, proporcionalidade e transparência.

Dessa forma, a regulamentação jurídica deve buscar um ponto de equilíbrio que permita a utilização econômica legítima dos dados pessoais sem desrespeitar os princípios constitucionais que asseguram a liberdade, a privacidade e a autodeterminação informativa. A construção de um modelo de monetização responsável, com proteção reforçada e mecanismos reais de controle pelo titular, representa uma via viável para compatibilizar inovação econômica com os direitos fundamentais no ambiente digital.

No campo da governança de dados, é essencial que o ordenamento jurídico tenha a capacidade de se adaptar rapidamente às transformações tecnológicas, garantindo que as práticas de coleta e comercialização respeitem os direitos fundamentais dos cidadãos. As práticas adotadas pelos *data brokers* podem impactar significativamente a proteção dos consumidores, sobretudo no que diz respeito à

privacidade e à autonomia. Entretanto, quando há uma regulamentação eficaz aliada a uma governança corporativa ética e transparente, torna-se possível fomentar inovação e geração de valor sem comprometer os direitos dos titulares dos dados.

Para preencher as lacunas regulatórias existentes, é fundamental que as legislações de proteção de dados evoluam de forma dinâmica e responsiva às rápidas mudanças tecnológicas. Isso requer um esforço conjunto entre governos, empresas e organizações da sociedade civil, com ênfase no fortalecimento dos mecanismos de fiscalização e na ampliação da transparência das práticas de coleta e uso de dados. Garantir que indivíduos estejam devidamente informados e protegidos é uma condição essencial para a construção de um mercado digital ético e sustentável.

Embora a conformidade com as leis de proteção de dados possa representar um desafio competitivo para empresas que dependem de dados pessoais para otimizar suas estratégias de negócio, quando os dados são utilizados de maneira responsável, com o devido consentimento e respeito à privacidade, as empresas podem conquistar vantagens competitivas, aumentar a confiança do consumidor e melhorar a personalização de serviços.

Em síntese, o equilíbrio entre inovação e proteção dos direitos individuais demanda um compromisso conjunto de todos os atores envolvidos no ecossistema digital. As empresas devem adotar uma abordagem ética e transparente no uso de dados, implementando tecnologias de privacidade desde sua concepção e cumprindo rigorosamente as regulamentações como a LGPD e o GDPR. Simultaneamente, os governos precisam assegurar que as normas sejam suficientemente ágeis e adaptáveis, permitindo que o progresso tecnológico ocorra sem comprometer os direitos fundamentais.

Por fim, conclui-se que é essencial que as organizações reconheçam os dados não apenas como ativos econômicos, mas como ativos empresariais estratégicos, que demandam um compromisso rigoroso com a proteção da privacidade e a promoção da cidadania digital. Integrar ética, inovação e conformidade legal nas práticas de tratamento de dados não apenas assegura o cumprimento das normas, mas também fortalece a competitividade sustentável das empresas. Dessa forma, aquelas que incorporarem esses princípios estarão mais preparadas para gerar valor duradouro e contribuir para a construção de um ambiente digital mais justo, transparente e

democrático. A criação de uma sociedade digital verdadeiramente sustentável depende do compromisso coletivo com a governança responsável dos dados.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Coleta de dados biométricos pela empresa Tools for Humanity**. Brasília: Ministério da Justiça e Segurança Pública, 2025. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/coleta-de-dados-biometricos-pela-empresa-tools-for-humanity>. Acesso em: 12 fev. 2025.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Jorge Zahar, 2013.

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

BRASIL. ANPD. **Autoridade Nacional de Proteção de Dados**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf. Acesso em: 10 out. 2024.

BRASIL. **Autoridade Nacional de Proteção de Dados**. Página institucional da ANPD. Disponível em: <https://www.gov.br/anpd/pt-br>. Acesso em: 10 nov. 2024.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**, Brasília, 11 fev. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**, Brasília, DF, 5 out. 1988.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF: **Presidência da República**, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406compilada.htm. Acesso em: 14 jan. 2015.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**, Brasília, 15 ago. 2018.

BRASIL. Lei nº 13.874, de 20 de setembro de 2019. Institui a Declaração de Direitos de Liberdade Econômica, estabelece garantias de livre mercado e dispõe sobre a primazia da interpretação jurídica favorável à liberdade econômica nas atividades privadas. **Diário Oficial da União**, Brasília, DF, 20 set. 2019.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.419.697/RS**, Relator: Ministro Paulo de Tarso Sanseverino 17 nov. 2014. Disponível em: <https://www.stj.jus.br/websecstj/cgi/revista/REJ.cgi/MON?seq=32791853>. Acesso em: 12 fev. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.758.799-MG**, Relatora Ministra Nancy Andrighi. 12 nov. 2019. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201700065219&dt_publicacao=19/11/2019. Acesso em: 12 fev. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 22.337-8/RS**, Relator Ministro Ruy Rosado Aguiar. 13 fev. 1995. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=199200114466&dt_pu. Acesso em: 12 fev. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 640.196 PR**, Relator: Ministro Castro Filho. 21 jun. 2005. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=200400431645&dt_publicacao=01/08/2005. Acesso em: 12 fev. 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e Territórios (TJDFT). **Agravo de Instrumento nº 0749765-29.2020.8.07.0000**. Rel. Des. Cesar Loyola. Brasília, DF, 2021. Disponível em: <https://pje2i.tjdft.jus.br>. Acesso em: 05 mar. 2025.

BUCTCHER, Isabel. **ANPD investiga coleta de dados biométricos da Tool for Humanity no Brasil**. Mobili Time, 2025. Disponível em: <https://www.mobiletime.com.br/noticias/15/01/2025/anpd-tools-for-humanity/>. Acesso em: 20 fev. 2025.

CAVOUKIEN, Ann. **Privacy by design: The 7 Foundational Principles**. Acesso em: 25 jan 2025.

CIPPIC – CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC. **On the data trail: how detailed information about you gets into the hands of organizations with whom you have no relationship**. Ottawa: University of Ottawa, Faculty of Law, 2006. Disponível em: <https://cippic.ca/sites/default/files/May1-06/Databrokers.pdf>. Acesso em: 22 maio 2025.

CONJUR. **Coleta de dados biométricos oculares no Brasil: implicações jurídicas, ética e riscos à privacidade**. Consultor Jurídico, 21 jan. 2025. Disponível em: <https://www.conjur.com.br/2025-jan-21/coleta-de-dados-biometricos-oculares-no-brasil-implicacoes-juridicas-etica-e-riscos-a-privacidade/>. Acesso em: 17 mar. 2025.

COSTA, Angélica Maria dos Santos; COSTA, Fernando Bartolomeu Mendonça. Proteção de dados pessoais na era tecnológica: desafios e responsabilidade civil. In: SILVA, Leide Jane Macedo (org.). **Perspectivas sobre a proteção de dados com ênfase nos desafios da advocacia**. São Paulo: Expert Editora, 2024. p. 41–42. Disponível em: <https://experteditora.com.br/wp-content/uploads/2024/05/Perspectivas-sobre-a-Protecao-de-Dados-com-enfase-nos-desafios-da-advocacia.pdf>. Acesso em: 22 jan 2025.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data: a revolução que vai transformar como vivemos, trabalhamos e pensamos**. 1. ed. Rio de Janeiro: Elsevier, 2013.

MAZIERO, Franco Giovanni Mattedi; SILVA, Leide Jane Macedo da. **A análise interpretativa da proporcionalidade no uso do legítimo interesse nas relações empresariais**. In: SILVA, Leide Jane Macedo da; BASTOS, Luciana de Castro (orgs.). Aspectos relevantes da Lei Geral de Proteção de Dados Pessoais. São Paulo: Expert Editora, 2021. p. 19–37. Disponível em: <https://experteditora.com.br/wp-content/uploads/2021/07/Aspectos-Relevantes-da-Lei-Geral-de-Prote%C3%A7%C3%A3o-de-Dados-Pessoais.pdf>. Acesso em: 10 set. 2024.

DGI. **Data Governance Institute**. [S.l.], 2021. Disponível em: <https://datagovernance.com/the-data-governance-basics/definitions-of-data-governance/>. Acesso em: 20 mar. 2025.

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

DONEDA, Danilo. **Proteção de dados**: fundamentos e perspectivas. São Paulo: Método, 2019.

DONEDA, Danilo. **Tratamento de dados pessoais: a função e os limites do legítimo interesse**. In: DONEDA, Danilo; MENDES, Laura Schertel (org.). Lei Geral de Proteção de Dados: comentada artigo por artigo. São Paulo: RT, 2021. p. 138-148.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the council. **Official Journal of the European Union**, 4 May 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 12 fev. 2025.

FEDERAL TRADE COMMISSION. **Data brokers**: a call for transparency and accountability. FTC, 2014. Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em: 12 fev. 2025.

FRAZÃO, Ana. **A nova economia digital**: tendências e modelos de negócio. São Paulo: Editora FGV, 2020.

GRIMALDI, Fabíola. **A importância criteriosa que a startup deve aplicar para atender o requisito do privacy by design da Lei Geral de Proteção de Dados**. In: SILVA, Leide Jane Macedo da (org.). Aspectos relevantes da Lei Geral de Proteção de Dados Pessoais. São Paulo: Expert Editora, 2021. p. 123–133. Disponível em: <https://experteditora.com.br/wp-content/uploads/2021/07/Aspectos-Relevantes-da-Lei-Geral-de-Prote%C3%A7%C3%A3o-de-Dados-Pessoais.pdf>. Acesso em: 22 maio 2025.

IBGC. **Instituto Brasileiro de Governança Corporativa**. [S.l.], 2021. Disponível em: <https://www.ibgc.org.br/quemsomos>. Acesso em: 20 mar. 2025.

JIMENEZ, Camila do Vale. Reflexões sobre Privacy by design e privacy by default: da idealização à positivação. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato (Coord). **Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia**. São Paulo: Ed. RT, 2018. Jimenez, Maldonado & Opice Blum, 2018.

JÚNIOR, Armando Kolbe. **Desafios estratégicos para a segurança e defesa cibernética**. 1. ed. Curitiba: Editora Intersaberes Ltda., 2020.

KRAEMER, Jan; SCHNURR, Daniel; HABERER, Bastian. **Do consumers benefit from selling their data?** The economic impact of personal data brokers on digital markets. TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy, 2018. 96 p. Última revisão: 19 dez. 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3141946. Acesso em: nov. 2024.

LESSIG, Lawrence. **Privacy as property**. Social Research, v. 69, n. 1, Spring 2002, pp. 250-3.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS (MPDFT) vs. SERASA S.A. **Ação Civil Pública nº 0736634-81.2020.8.07.0001**. Tribunal de Justiça do Distrito Federal e Territórios, 2020. Disponível em: <https://www.tjdft.jus.br>. Acesso em: 18 abr 2025.

OLAVSRUD, T. **What is data governance?** A best practices framework for managing data assets. [S. l.], 2020.

PIMENTA, Eduardo Goulart. **Estrutura jurídica da empresa na era digital**. São Paulo: Expert Editora Digital, 2022. Disponível em: <https://experteditora.com.br/estrutura-juridica-da-empresa-na-era-digital>. Acesso em: 07 fev. 2025.

PINHEIRO, Patricia Peck. **Direito digital**. 6ª edição. São Paulo: Saraiva, 2018.

POSNER, Richard. **Economic analysis of law**. 7th ed. New York: Wolters Kluwer Law & Business, 2007.

PROCON-SP pede explicações da Tools for Humanity sobre escaneamento de íris. **Exame**, 14 fev. 2025. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/coleta-de-dados-biometricos-pela-empresa-tools-for-humanity>. Acesso em: 20 fev. 2025.

QUINTILIANO, Leonardo. Posso vender meus dados pessoais? O resgate da doutrina da privacidade como propriedade. **Migalhas**, 25 nov. 2022. Disponível em: <https://www.migalhas.com.br/columa/migalhas-de-protecao-de-dados/377587/posso-vender-meus-dados-pessoais>. Acesso em: 12 fev. 2025.

RODOTÀ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

ROSSETTI, José Paschoal. **A empresa e seu ambiente de interação**: os limites da Teoria dos Custos de Transação e o alcance da Teoria Institucionalista Evolucionária. *Ecos - Revista Científica da Economia*, Campinas, v. 26, n. 2, p. 1–20, 2020. Disponível em: <https://www.scielo.br/j/ecos/a/W6ms6VK3vGzGLwcTDL3xgKc/?lang=pt>. Acesso em: 17 fev 2025.

SAMPAIO, Alice Castaldi. **Data brokers**: um novo modelo de negócios baseado em vigilância de dados. 2017. Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Estudos da Linguagem, Campinas, SP, 2017.

STANLAKE. George Frederik. **Introdução à Economia**. Lisboa: Fundação Calouste Gulbenkian, 1993. p 95

UNIVERSIDADE DE COIMBRA. **Avaliação de Impacto sobre a Proteção de Dados (DPIA)**, Lisboa: UC, 2017. Disponível em: <https://www.uc.pt/protecao-de-dados-e-informacao-administrativa/protecao-de-dados-pessoais/aipd/>. Acesso em: 12 fev. 2025.

VALADÃO, Rodrigo Borges. **Monetização dos dados pessoais: a nova fronteira da privacidade**. 2025. Disponível em: https://www.academia.edu/129225001/Monetiza%C3%A7%C3%A3o_dos_Dados_Pessoais_A_Nova_Fronteira_da_Privacidade. Acesso em: 14 mai 2025.

ZANATTA, Rafael; SECAF, Helena; MENDONÇA, Julia. A aplicabilidade da Lei Geral de Proteção de Dados Pessoais aos corretores de dados, in: VILLAS BOAS CUEVA, Ricardo; FRAZÃO, Ana. **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters, 2021, p. 957-988.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. New York: Public Affairs, 2018.