UNIVERSIDADE FEDERAL DE GOIÁS
CÂMPUS GOIÁS
FACULDADE DE DIREITO

DURVAL MESSIAS DE JESUS

OS DESAFIOS DA EFETIVAÇÃO DO DIREITO À PRIVACIDADE DIGITAL NO BRASIL: PROTEÇÃO DE DADOS PARA ALÉM DO CONSENTIMENTO, UMA ANÁLISE À LUZ DA LEI 13.709/2018

GOIÁS-GO
2024

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome completo do autor: Durval Messias de Jesus

Título do trabalho: Os desafios da efetivação do direito à privacidade digital no Brasil: proteção de dados para além do consentimento, uma análise à luz da Lei 13.709/2018

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [x] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Durval Messias De Jesus**, **Discente**, em 03/01/2025, às 10:55, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Jose Humberto De Goes Junior**, **Professor do Magistério Superior**, em 03/01/2025, às 10:57, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5045579** e o código CRC **3FB9CA3A**.

Referência: Processo nº 23070.064145/2024-96 SEI nº 5045579

DURVAL MESSIAS DE JESUS

Os desafios da efetivação do direito à privacidade digital no Brasil: proteção de dados para além do consentimento, uma análise à luz da Lei 13.709/2018

Trabalho apresentado como requisito parcial para obtenção do título de Bacharel em Direito pela Universidade Federal de Goiás.

Orientador: Dr. José Humberto de Góes Junior.
Coorientadora: Dra. Bruna Pinotti Garcia.

GOIÁS-GO
2024

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Jesus, Durval Messias de
Os desafios da efetivação do direito à privacidade digital no Brasil [manuscrito] : proteção de dados para além do consentimento, uma análise à luz da lei 13.709/2018 / Durval Messias de Jesus. - 2024.
106 f.

Orientador: Prof. Dr. José Humberto de Góes Junior; co-orientador Dr. Bruna Pinotti Garcia.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Sociais Aplicadas, Direito, Cidade de Goiás, 2024.

Inclui siglas.

1. Privacidade digital. 2. Proteção de dados pessoais. 3. Lei Geral de Proteção de Dados (LGPD). 4. Consentimento. 5. Sociedade da informação e vigilância. I. Góes Junior, José Humberto de, orient. II. Título.

CDU 34

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos dezessete dias do mês de dezembro do ano de dois mil e vinte e quatro, às 16h, de forma híbrida, iniciou-se a sessão pública de defesa do Trabalho de Conclusão de Curso (TCC) intitulado **"Os desafios da efetivação do direito à privacidade digital no Brasil: proteção de dados para além do consentimento, uma análise à luz da Lei 13.709/2018"**, de autoria de **Durval Messias de Jesus**, do curso de Direito, da Unidade Acadêmica Especial de Ciências Sociais Aplicadas do Câmpus Goiás da UFG. Os trabalhos foram instalados pelo Professor Doutor. José Humberto de Góes Junior – orientador (UAECSA/UFG) – e pela Professora Doutora Bruna Pinotti Garcia – coorientadora (UAECSA/UFG) –, com a participação dos demais membros da Banca Examinadora: Professora Doutora Maria Carolina Carvalho Motta e Professor Doutor Vitor Sousa Freitas. Posteriormente, a Banca Examinadora reuniu-se reservadamente e considerou o trabalho **APROVADO COM INDICAÇÃO PARA PUBLICAÇÃO**.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Jose Humberto De Goes Junior**, **Professor do Magistério Superior**, em 03/01/2025, às 10:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Maria Carolina Carvalho Motta**, **Professor do Magistério Superior**, em 06/01/2025, às 15:32, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Vitor Sousa Freitas**, **Professor do Magistério Superior**, em 08/01/2025, às 15:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

Documento assinado eletronicamente por **Bruna Pinotti Garcia**, **Professora do Magistério Superior**, em 09/01/2025, às 20:16, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020 .

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5045578** e o código CRC **76D0AD09**.

Referência: Processo nº 23070.064145/2024-96 SEI nº 5045578

AGRADECIMENTOS

Agradeço, primeiramente, à minha família, especialmente à minha mãe, minha maior referência. Foi ela quem me proporcionou, não apenas o suporte financeiro, mas principalmente o emocional necessário para o meu desenvolvimento intelectual. Foi ela quem me ensinou a ler, me incentivou na escolha deste curso e nunca permitiu que eu desistisse de nada. Sua força, coragem e exemplo me mostraram que o impossível só existe para quem acredita nele. Ela me inspirou a ser a minha melhor versão e, por isso, dedico a ela não apenas esta monografia, mas todas as conquistas que me trouxeram até aqui.

Aos meus amigos, agradeço por sempre acreditarem em mim e me incentivarem ao longo desta jornada. Em especial, à Duda, ao Keven Moraes e ao João Pedro, que estiveram ao meu lado, compartilhando desafios e vitórias, e que comigo abriram e encerraram este ciclo de formação.

À minha namorada, amiga e colega de classe, Júlia, minha eterna gratidão por tudo que fez por mim durante a graduação. Ao seu lado, tudo se tornou mais leve. Obrigado pelas risadas, pelo carinho, pelo cuidado e por sempre me motivar a evoluir, tanto no âmbito pessoal quanto acadêmico.

Agradeço também aos meus orientadores. À Bruna Pinotti, pela inspiração na escolha do tema e pela influência positiva nas decisões que tomaram forma nesta monografia. E ao meu orientador e amigo, José Humberto, pelas valiosas instruções, conselhos e experiências compartilhadas e proporcionadas. Sua dedicação e trabalho não apenas me orientaram, mas também aumentaram minha admiração pelo Direito e meu desejo de aprofundar-me na área.

Por fim, agradeço à UFG, a todos os professores, profissionais da administração e da zeladoria, pelo ambiente acolhedor que proporcionaram. Aos colegas da universidade e a cada pessoa que contribuiu direta ou indiretamente para a conclusão desta monografia, dedico meu mais profundo agradecimento. Esta conquista é também fruto do apoio e da colaboração de todos vocês.

RESUMO

A presente monografia aborda os desafios da efetivação do direito à privacidade digital no Brasil, com foco na proteção de dados pessoais além do consentimento, sob a perspectiva da Lei Geral de Proteção de Dados (Lei nº 13.709/2018). Inicialmente, contextualiza-se a transição histórica das sociedades, desde a agrícola até a "sociedade da informação", destacando a centralidade da informação como ativo econômico e instrumento de poder na contemporaneidade. Nesse contexto, os dados pessoais são analisados como extensão da personalidade humana, demandando uma abordagem normativa que promova a dignidade, a autonomia e a autodeterminação informativa dos indivíduos. A pesquisa identifica as limitações do modelo centrado no consentimento, especialmente diante das assimetrias informacionais e do aumento da vigilância tecnológica. Além disso, examina-se o impacto das novas tecnologias na construção de perfis comportamentais e nos riscos de discriminação algorítmica, evidenciando a hipervulnerabilidade dos titulares de dados. Por fim, a monografia propõe uma abordagem sistêmica para a proteção de dados pessoais, fundamentada na regulação por riscos, com foco em princípios dinâmicos e na superação da dicotomia entre público e privado. Tal proposta reflete a necessidade de adaptar o ordenamento jurídico brasileiro aos desafios éticos e jurídicos impostos pela economia digital e pela dataficação das relações sociais, consolidando os dados como uma categoria autônoma de direitos da personalidade.

Palavras-chave: Privacidade digital; Proteção de dados pessoais; Lei Geral de Proteção de Dados (LGPD); Consentimento; Sociedade da informação e vigilância.

ABSTRACT

This dissertation addresses the challenges of enforcing the right to digital privacy in Brazil, focusing on data protection beyond consent under the framework of the General Data Protection Law (Law No. 13,709/2018). Initially, it contextualizes the historical transition of societies, from agricultural to the information society, emphasizing the centrality of information as an economic asset and instrument of power in contemporary times. In this context, personal data is analyzed as an extension of human personality, requiring a normative approach that promotes dignity, autonomy, and informational self-determination. The research identifies the limitations of the consent-centered model, especially considering informational asymmetries and the rise of technological surveillance. Furthermore, it examines the impact of new technologies on behavioral profiling and the risks of algorithmic discrimination, highlighting the hyper-vulnerability of data subjects. Finally, the dissertation proposes a systemic approach to personal data protection based on risk regulation, focusing on dynamic principles and overcoming the dichotomy between public and private spheres. This proposal reflects the need to adapt Brazilian legal frameworks to the ethical and legal challenges posed by the digital economy and the datafication of social relations, consolidating data as an autonomous category of personality rights.

Keywords: Digital privacy; Personal data protection; General Data Protection Law (LGPD); Consent; Information society and Surveillance.

Lista de Abreviaturas e Siglas

ABCOMM – Associação Brasileira de Comércio Eletrônico

ANPD - Autoridade Nacional de Proteção de Dados

CC – Código Civil

CDC – Código de Defesa do Consumidor

CF – Constituição Federal

CNJ – Conselho Nacional de Justiça

FTC – *Federal Trade Commission* (Comissão Federal de Comércio dos Estados Unidos)

GDPR – *General Data Protection Regulation* (Regulamento Geral de Proteção de Dados da União Europeia)

IBGE – Instituto Brasileiro de Geografia e Estatística

IA – Inteligência Artificial

IoT – Internet of Things (Internet das Coisas)

LGPD – Lei Geral de Proteção de Dados

MCI – Marco Civil da Internet

ONU – Organização das Nações Unidas

PNAD – Pesquisa Nacional por Amostra de Domicílios

RIPD – Relatório de Impacto à Proteção de Dados

SEBRAE – Serviço Brasileiro de Apoio às Micro e Pequenas Empresas

TIC – Tecnologias da Informação e Comunicação

SUMÁRIO

INTRODUÇÃO

A privacidade digital, reconhecida como um direito fundamental em um mundo cada vez mais interconectado assume uma posição central nos debates sobre justiça social, desenvolvimento econômico e proteção de direitos individuais na "sociedade da informação". Essa sociedade, marcada pela convergência tecnológica e pela dataficação das relações humanas, transformou a informação em um ativo estratégico, impulsionando a economia digital e intensificando o poder de atores que controlam o fluxo e o uso de dados. No entanto, esse avanço tem gerado profundas assimetrias informacionais e de poder, que colocam em risco direitos fundamentais, como a autodeterminação informativa e a dignidade humana, ao mesmo tempo em que redefinem os contornos do conceito de privacidade.

O advento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), aqui referida como LGPD, no ordenamento jurídico brasileiro, representa uma tentativa de regular essa nova realidade, fornecendo um arcabouço normativo que visa equilibrar interesses econômicos e sociais, além de oferecer proteção aos dados pessoais em um ambiente de constante inovação tecnológica. Embora estabeleça princípios e direitos relevantes, como o da transparência e da segurança, a LGPD ancora-se predominantemente no consentimento como fundamento central para o tratamento de dados, o que, em face das práticas contemporâneas de vigilância pervasiva e do *big data*, revela-se insuficiente. A assimetria de poder e conhecimento entre usuários e as entidades que controlam a coleta e o processamento de dados mina a eficácia do consentimento, comprometendo a autonomia dos titulares e expondo vulnerabilidades que transcendem a simples relação contratual.

Essa lacuna regulatória ganha relevância à medida que as tecnologias de informação e comunicação (TICs) promovem a coleta massiva de dados, frequentemente realizada de forma invasiva e opaca. As implicações disso vão desde a construção de perfis comportamentais e a discriminação algorítmica até a manipulação de preferências e comportamentos por meio de sistemas baseados em *machine learning*. Nesse contexto, os dados pessoais deixam de ser simples informações sobre indivíduos para se tornarem uma extensão de sua personalidade, uma projeção digital da identidade que merece proteção jurídica robusta. A inadequação do modelo de consentimento como pilar regulatório central evidencia a necessidade de se adotar abordagens mais abrangentes, como a regulação baseada em riscos, que considera não apenas as consequências individuais do uso de dados, mas também os impactos coletivos e sistêmicos.

Essa perspectiva é particularmente importante quando se considera que a privacidade, no contexto atual, não é apenas um direito individual, mas também um bem coletivo essencial à preservação de uma sociedade democrática. A invasão da privacidade compromete não apenas a autodeterminação informativa, mas também a equidade e a justiça social, pois as práticas de vigilância e a comercialização indiscriminada de dados reforçam desigualdades preexistentes e criam novas formas de opressão. Além disso, o uso indevido de dados para discriminação algorítmica, seja em processos de crédito, recrutamento ou acesso a serviços públicos, ilustra como a tecnologia pode perpetuar e aprofundar preconceitos históricos, afetando desproporcionalmente grupos já vulneráveis.

Diante desses desafios, esta monografia propõe uma análise crítica e aprofundada das barreiras à efetivação do direito à privacidade digital no Brasil, com foco na superação das limitações do consentimento como princípio basilar da proteção de dados pessoais. Para tanto, adota-se uma abordagem interdisciplinar, que inclui a análise histórica das transformações sociais e econômicas até a consolidação da "sociedade da informação", a avaliação crítica do impacto das TICs na construção de novos paradigmas de vigilância e discriminação, e o exame das contribuições teóricas e normativas para a proteção de dados no Brasil e no mundo.

A investigação avança ao propor uma abordagem regulatória fundamentada no conceito de regulação por riscos, que privilegia a análise de impactos e a adoção de medidas proativas para mitigar os danos associados ao uso inadequado de dados pessoais. Além disso, destaca-se a necessidade de reconhecer os dados pessoais como uma categoria autônoma de direitos da personalidade, transcendendo a dicotomia entre público e privado para incorporar uma visão mais sistêmica da proteção de dados. Essa perspectiva, alinhada às melhores práticas internacionais e às contribuições teóricas de autores como Stefano Rodotà e Daniel Solove, busca adaptar o ordenamento jurídico brasileiro às demandas éticas e tecnológicas da sociedade contemporânea.

Por fim, esta monografia não se limita a identificar falhas no modelo vigente, mas apresenta propostas concretas para a evolução da legislação e da jurisprudência no Brasil. A pesquisa reforça a importância de um marco regulatório que reconheça a privacidade como um bem coletivo e sistêmico essencial à dignidade humana e ao equilíbrio de poder na sociedade da informação. Com isso, contribui para o debate acadêmico e jurídico ao propor soluções inovadoras que promovam a igualdade informacional, a justiça social e a proteção efetiva dos direitos fundamentais em um cenário de rápidas transformações tecnológicas e sociais.

CAPÍTULO 1 - O DESPERTAR DE UMA NOVA ERA: A SOCIEDADE DA INFORMAÇÃO

A trajetória das sociedades humanas no contexto europeu ocidental é marcada por transformações estruturais que redefiniram suas bases econômicas, culturais e tecnológicas. Essas mudanças refletem dinâmicas de poder e a adaptação às novas oportunidades e necessidades, seja por meio do avanço tecnológico ou de reorganizações políticas (Le Goff, 2005, p. 191-256).

Embora cada época tenha compreendido uma lógica predominante, diferentes modelos de produção e organização coexistiram ao longo do tempo. Le Goff (2005, p. 325-363) observa, por exemplo, que mesmo com a transição da economia medieval para o capitalismo nascente, impulsionada pelos avanços comerciais e urbanos, a agricultura e sistemas produtivos locais continuaram a desempenhar um papel fundamental. Assim, formas mais rudimentares de produção seguem concorrendo com sistemas mais complexos e integrados, como o industrial.

Nesse sentido, diante da multiplicidade de sistemas coexistentes na contemporaneidade, um novo modelo de organização social[1] emerge como sendo o dominante, tendo a informação como principal ativo, estruturando uma nova sociedade, centrada no conhecimento e nas tecnologias da informação e comunicação (TICs) (Bioni, 2021, p. 04). As estruturas econômicas e sociais, antes orientadas por fatores tangíveis como a terra e o capital, se depararam com uma nova estrutura socioeconômica concorrente, que no intangível da informação e de seu processamento, progressivamente tem alterado as dinâmicas de poder e desenvolvimento[2].

Esse novo cenário levanta questões sobre o controle e o uso da informação, especialmente no que tange à privacidade e à concentração de poder em torno dos dados. Embora a "sociedade da informação" traga avanços econômicos e tecnológicos, ela também introduz desafios éticos e jurídicos. A história das sociedades precedentes ajuda a entender como a informação se tornou central nas relações econômicas e sociais, mas também ilumina os riscos inerentes a essa nova dinâmica, como o aumento da vigilância, desigualdade e vulnerabilidade.

---

[1] Esta expressão é utilizada por Daniel Militão da Silva (2009) em sua dissertação de mestrado "Desafios do ensino jurídico na pós-modernidade: da sociedade agrícola e industrial para a sociedade da informação".

[2] De acordo com Peter Drucker (1993), os tradicionais fatores de produção, como terra, mão de obra e capital, continuam existindo, mas passaram a ocupar uma posição secundária. Esses fatores podem ser facilmente obtidos, desde que se tenha conhecimento, que assume um papel central ao ser visto como algo útil e um meio para a obtenção de resultados sociais e econômicos.

Com essas mudanças, emerge a necessidade de refletir criticamente sobre as implicações desse novo modelo, em que os dados não são apenas motores de inovação, mas também instrumentos de poder e controle.

1.1 AS SOCIEDADES: AGRÍCOLA, INDUSTRIAL E A DA INFORMAÇÃO

O tempo e a história caminham lado a lado[3] e podem ser examinados das mais diferentes perspectivas. A humanidade se relaciona de diversas formas com o tempo e, no curso da história, essas relações se alteraram ou permaneceram inalteradas em diferentes culturas[4] (Silva, 2009, p. 09).

Podemos invocar como exemplos culturas milenares, especialmente em povos do oriente em que muitas vezes o tempo é julgado de forma cíclica com a sucessão de acontecimentos que tendem a repetir o mesmo percurso, invariavelmente, em uma espécie de "eterno retorno"[5], ao contrário de outras culturas, cuja concepção da história apresenta uma visão mais linear tendente a uma evolução e um ponto culminante.

São muitas as formas de se observar e segmentar o tempo. Toma-se para fins desta monografia a perspectiva ocidental naquilo que concerne à periodização e a seleção dos momentos mais relevantes para a identificação de transição dos períodos históricos. Sob esta ótica, percebe-se que a sociedade ocidental, no curso de sua formação se deparou com

---

[3] Falar sobre a história e o tempo não é uma tarefa simples. Muito pertinente é a questão colocada por Santo Agostinho (1984, p. 338) em reflexão sobre o tempo: "O que é o tempo? Se ninguém me pergunta, eu sei; mas se alguém me pergunta e eu quero explicar, já não sei mais". Nesse sentido, o tempo e a história caminham juntos e podem ser examinados sob diversas perspectivas (Silva, 2009). Nesta monografia, adota-se uma perspectiva ocidental, linear e evolutiva, que estrutura a história em fases de desenvolvimento social e econômico. Como observado por Raquel Glezer (2002), essa abordagem eurocêntrica frequentemente segmenta o tempo em períodos que refletem mudanças estruturais, baseando-se em temporalidades adequadas aos fenômenos em análise, seja em uma longa duração para estruturas sociais e mentalidades ou em temporalidades curtas e factuais para eventos políticos e econômicos.

[4] A relação da humanidade com o tempo varia conforme o contexto cultural. Nas tradições orientais, como na cultura hindu e budista, o tempo é frequentemente entendido de maneira cíclica, com ciclos repetitivos de criação, destruição e renascimento (*samsara*) (Smith, 2009, p. 75). Em contrapartida, a visão ocidental, fortemente influenciada pelo cristianismo, adota uma perspectiva linear, na qual a história avança progressivamente em direção a um objetivo final, como o juízo final ou a salvação (Le Goff, 2005). Essas concepções distintas influenciam diretamente a forma como cada cultura interpreta e registra o desenvolvimento histórico.

[5] O eterno retorno é uma teoria que propõe que o universo e toda a existência se repetem infinitamente em ciclos ao longo do tempo ou do espaço. Esse conceito é encontrado em diversas tradições filosóficas e religiosas, como na filosofia indiana, no Egito antigo, no Eclesiastes judaico e foi adotado por pitagóricos e estoicos. Com o advento do cristianismo, o conceito perdeu força no Ocidente, exceto na filosofia de Friedrich Nietzsche no século XIX, que o relacionou a outros de seus conceitos, como o *amor fati*. O eterno retorno também se associa à ideia de pré-determinismo, sugerindo que as pessoas repetem eternamente os mesmos eventos. Scarlett Marton (2000) faz várias referências a filosofias e a tradições religiosas da antiguidade que teriam expressado a doutrina.

diversasformas de organização social[6], tendo cada qual, um elemento central para o seu desenvolvimento, sendo o modo pelo qual ele se estruturou o fator determinante para se estabelecer os seus respectivos marcos históricos.

Na sociedade agrícola, a fonte de riquezas provinha mais especificamente da terra. Nesse contexto, o produto agrícola emerge como elemento central dessa economia, que por meio da prática do escambo, constituiu a primeira prática comercial[7] (Bioni, 2021).

Posteriormente, na Europa e nos Estados Unidos[8], a máquina a vapor e a eletricidade despontam como elementos centrais na produção fabril e, consequentemente, na produção de riquezas (sociedade industrial) (Silva, 2009).

Com a consolidação da era industrial a humanidade assegurou o domínio básico das necessidades de sobrevivência – bens materiais como comida e abrigo[9]. Em um terceiro momento, o desenvolvimento –, uma vez que, o amplo avanço da técnica e da ciência passou a moldar a sociedade atual, conhecida como "sociedade da informação"[10] (Silva, 2009).

Essa nova forma de organização social foi consolidada em decorrência dos avanços tecnológicos recentes, que criaram mecanismos capazes de processar e transmitir informações em uma quantidade e velocidade jamais prospectada. Houve assim, uma nova forma de se relacionar com o espaço-tempo visto que, no plano *online* as interações se dão de forma imediata (Bioni, 2021).

---

[6] Esta expressão é utilizada por: Daniel Pereira Militão Silva (2009).

[7] A agricultura permanece como um dos pilares da balança comercial brasileira, representando mais de 45% das exportações em 2023, com destaque para produtos como soja, milho e carne bovina (BRASIL, 2023). Nesse sentido, o Brasil continua inserido predominantemente no contexto de uma "sociedade agrícola" na Divisão Internacional do Trabalho, devido ao processo de reprimarização de sua economia, que reforça sua posição como exportador de *commodities*, em detrimento de uma industrialização mais robusta. Esse cenário reflete a dependência excessiva do setor primário, o que limita a capacidade do país de desenvolver cadeias produtivas mais complexas e de maior valor agregado, perpetuando sua posição periférica (Carneiro, 2015).

[8] A industrialização se desenvolveu primeiro na Europa Ocidental e nos Estados Unidos (Lopes, 2008).

[9] Karl Polanyi (2000), em sua obra "A grande transformação", argumenta que a consolidação da era industrial reorganizou os meios de subsistência humana ao transformar trabalho e terra em mercadorias. Esse processo permitiu atender às necessidades materiais básicas, como alimentação e moradia, porém, ao subordinar esses recursos essenciais às leis do mercado, o sistema gerou desequilíbrios econômicos e sociais.

[10] O termo "sociedade da informação" foi cunhado pelo sociólogo japonês Yoneji Masuda (1980). Em sua obra "*The informationsociety as post-industrialsociety*", Masuda explorou como a transição de uma sociedade industrial para uma sociedade baseada em informações e tecnologias transformaria as estruturas econômicas e sociais.

Diante desse novo contexto[11], ainda que essa nova forma de organização social não se resuma apenas ao meio ambiente virtual[12], a computação eletrônica e a *internet* são as ferramentas de destaque desse processo.

1.2 ECONOMIA DA INFORMAÇÃO

A economia da informação caracteriza-se pela centralidade dos dados e da informação como recursos essenciais ao desenvolvimento econômico. Nesse contexto, o valor econômico é gerado pelo processamento e transformação da informação em conhecimento aplicado, utilizado para otimizar processos e promover inovação em diferentes setores (Amaral, 2009, p. 116).

Com o avanço das Tecnologias da Informação e Comunicação (TICs), tornou-se possível a coleta, o armazenamento e o processamento massivo de dados. Isso transformou profundamente a maneira como as empresas operam, permitindo tomadas de decisão mais assertivas, identificação de padrões de consumo e desenvolvimento de produtos com maior precisão (Drucker, 1993). A informação, portanto, deixa de ser um recurso passivo e se torna um ativo estratégico, gerando vantagens competitivas.

A transição do ambiente analógico para o digital, viabilizada pela *internet* e outras inovações tecnológicas, criou um mercado global interconectado, por meio de que a troca e o uso eficiente de dados são fundamentais (Castells, 2002). Nesse novo cenário, a informação assume o papel de matéria-prima essencial, fomentando um mercado baseado na sua coleta, análise e comercialização. Nos próximos itens, será abordado como a virtualização e a dataficação da informação transformaram-na em matéria-prima central para a nova economia. Esses processos, embora possibilitem maior eficiência e novas oportunidades de mercado, também levantam questões importantes sobre privacidade, controle de dados e desigualdades no acesso e uso da informação, refletindo tanto benefícios quanto desafios desse novo cenário econômico.

[11] As sociedades agrícola, industrial e da informação coexistem, sem se superarem totalmente. No Brasil, a reprimarização da economia mostra a persistência da agricultura, mesmo com avanços rumo à sociedade da informação. A "sociedade da informação" convive com modelos anteriores, refletindo a sobreposição de diferentes temporalidades e formas de organização social.

[12] A "sociedade da informação" compreende todo e qualquer tipo de acesso facilitado, como *fax*, ligações,etc.

1.2.1 A virtualização da informação e a sua subsequentemente datificação

A consolidação da "sociedade da informação" está diretamente ligada ao avanço na capacidade de processamento de dados, impulsionado pela descoberta dos *bits*[13]. Esses elementos fundamentais, representados pelo sistema binário (0 e 1), permitem que os computadores armazenem grandes volumes de informação em formato digital. Essa estrutura não apenas facilita o armazenamento, mas também possibilita o processamento rápido e a execução de comandos pré-determinados, como a busca de informações através de palavras-chave, tornando o acesso e a manipulação de dados muito mais eficientes.

Os *bits* desmaterializam a informação, permitindo a sua inserção em computadores. É nesse sentido que, frequentemente se faz referências aos quatro v's do *big data*[14]: os computadores atuais processam dados de forma mais veloz, veraz, variada e volumosa (Frazão, 2019). Como consequência, nota-se, uma guinada quantitativa e qualitativa no que concerne à capacidade de processamento de dados, visto que, respectivamente, aumentou-se o poder de processamento – por conseguinte, mais dados são processados e, também, em menos tempo –, enquanto paralelamente, operou-se a sofisticação das técnicas de processamento - possibilitando a obtenção de dados mais pertinentes (Doneda, 2019).

Nota-se que não são criados novos dados. Apenas foram criadas ferramentas que permitem mensurar informações – sejam elas números, comportamentos, etc. – e estruturá-las em formatos que possibilitem seu uso em prol das mais distintas finalidades. A esse fenômeno se convencionou chamar de "dataficação"[15].

Como consequência à "dataficação" e a esse novo contexto do *big data*, toda e qualquer informação, ainda que considerada fútil, pode se tornar útil, o que implica que toda informação carece de proteção. Portanto, torna-se possível a conversão de uma informação dispersa em uma informação organizada (Doneda, 2019), o que implicou na plena reformulação da

---

[13] De acordo com Houaiss e Villar (2009), o dígito binário é definido como a menor unidade de informação processada por um computador, além de se referir ao algarismo do sistema binário que pode assumir apenas os valores 0 ou 1.

[14] *Big data* é um conjunto de dados maior e mais complexo, especialmente de novas fontes de dados. Esses conjuntos de dados são tão volumosos que o *software* tradicional de processamento de dados simplesmente não consegue gerenciá-los.

[15] Viktor Mayer-Schönberger e Kenneth Cukier (2013) foram responsáveis por popularizar o termo "dataficação", conceituando-o como o processo de converter aspectos do comportamento humano em dados digitais, que podem ser armazenados, analisados e utilizados para gerar *insights*. Essa transformação é vista como uma consequência direta do avanço das tecnologias digitais e do *big data*, possibilitando novas formas de criação de valor a partir de dados antes inquantificáveis.

disciplina jurídica da informação em razão do desenvolvimento da informática (Doneda, 2019),a ser discutida de forma mais aprofundada em um capítulo futuro (*Vide Capítulo 1.3*).

1.2.2 Informação como matéria-prima de uma nova economia

É natural inferir que, de uma "sociedade da informação", emerja concomitantemente uma "economia da informação". Com a possibilidade de organizar dados de maneira mais escalável (*e.g.,big data*), nasce um mercado cuja matéria-prima é o próprio cidadão ou, mais precisamente, seus dados.

A informação é central em um (novo) contexto econômico que busca gerar um conhecimento[16] capaz de viabilizar o empreendedorismo de forma mais eficiente no mercado – *marketing*[17]. Nota-se, que a informação em si não é o que alavanca eficiência na atividade empresarial, mas o seu processamento-organização a ser transformado em um conhecimento[18].

Antes mesmo da criação da *internet*, o papel central da informação já era reconhecido como essencial para o desenvolvimento econômico. Um exemplo marcante disso é o "gênero cartográfico portulano*"*, elaborado entre os séculos XIII e XV, que passou a representar com precisão as distâncias e rotas entre portos na bacia do Mediterrâneo. Sua criação foi motivada pelo renascimento do comércio marítimo, especialmente após as Cruzadas, que resultaram na coleta de grandes quantidades de informações geográficas da região (Nogueira; Biasi, 2015). Esses dados, antes dispersos, foram organizados e transformados em um recurso valioso para navegadores e comerciantes da época. O "mapa portulano" não apenas facilitou a criação de rotas marítimas mais eficientes, mas também se tornou um marco no uso da informação como ferramenta para gerar conhecimento e impulsionar o comércio.

Ao longo da história, encontram-se diversos outros exemplos que demonstram como o uso da informação foi essencial para o progresso econômico e tecnológico. No entanto, a

[16] Comumente, informação e conhecimento se confundem, nesse sentido, a informação pode ser definida como dados processados sobre alguém ou alguma coisa, enquanto o conhecimento refere-se a informações úteis obtidas através da aprendizagem e da experiência, ou seja, o conhecimento acontece, quando a informação é processada.
[17] De acordo com Philip Kotler (2000), o *marketing* pode ser definido como o processo social em que indivíduos e grupos satisfazem suas necessidades e desejos por meio da criação, oferta e livre negociação de produtos e serviços de valor com outros.
[18] Segundo João Ferreira do Amaral (2009), o que realmente gera valor para uma empresa não é simplesmente a aquisição de informações, mas a sua transformação em conhecimento que depois é aplicado. Ele ressalta a importância de se discutir o processo de conversão da informação em conhecimento dentro das dinâmicas empresariais.

transição do analógico para o digital[19] trouxe uma mudança ainda mais profunda. A elevação dos dados como o elemento central para o desenvolvimento econômico é a ímpar consequência deste fenômeno. O sociólogo Manuel Castells (2005), faz importantes reflexões quanto a esse novo terreno histórico, definido por ele como "sociedade em rede", que, "em termos simples, é uma estrutura social baseada em redes operadas por TICs fundamentadas na microeletrônica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessa rede".

Manuel Castells (2003) aponta para o que se convencionou chamar de globalização[20], contexto no qual as redes de comunicação digital formam a espinha dorsal de uma nova sociedade. Essa sociedade opera com base na interconectividade global e na flexibilidade para se reconfigurar, interligando diversos atores distribuídos pelos nós dessa vasta rede. Dentro desse panorama, existem muitas práticas que dão sentido à rede. No entanto, este estudo focará nos modelos de empresas organizadas em rede[21], que são responsáveis por estabelecer uma nova dinâmica na geração de riquezas (Castells, 2003).

Admite-se, com o objetivo de ilustrar o que se chama de "sociedade em rede" acima indicada, a seguinte exemplificação: em uma economia globalizada, uma multinacional como a Nike, pretendendo atender o mercado global no segmento de vestuário, descentraliza seu processo de fabricação e logística em um conjunto de empresas[22], que atuam de maneira colaborativa, a partir de uma função pré-estipulada (Castells, 2003, p. 58).

Isto é, a Nike basicamente processa informações. Analisando tendências do mercado e de suas próprias vendas – informação –, a empresa estadunidense pode avaliar qual produto não é eficiente no mercado – conhecimento –, oportunizando-se, portanto, a (re)projeção de um

[19] Aqui cabe lembrar que a LGPD se aplica também aos meios digitais e não somente a eles. Se se observa o artigo primeiro da lei, será possível perceber isso: "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." (sem grifos no original).

[20] Para Manuel Castells (2005), globalização e sociedade em rede seriam sinônimos, porém a ideia de globalização seria na sua concepção mais descritiva e menos analítica do que se pode esperar do conceito de sociedade em rede.

[21] A "sociedade em rede" pode se manifestar, também, na sociabilidade, na cultura e identidade, política, trabalho e produção etc. (*Ibidem*).

[22] Manuel Castells (2003) explica que a organização em rede se dá pela cooperação temporária entre diferentes empresas para a execução de um projeto específico, reconfigurando suas conexões conforme a necessidade. Um exemplo desse modelo é a Nike, que vendeu suas operações na Argentina, Chile e Uruguai ao Grupo Axo em 2020, demonstrando a flexibilidade empresarial em ajustar suas redes conforme as demandas de mercado (Ryngelblum, 2020).

determinado produto que tende a ser amplamente aceito pelo mercado a ser transmitido às demais empresas que compõem a rede[23], em especial às que competem o processo fabril.

Uma convergência de fatores é o que organiza uma nova dinâmica econômica, ao alocar o fluxo informacional como determinante no ciclo econômico, sobrepondo-se a qualquer outro meio de produção (Lisboa, 1995). Como consequência, é natural inferir que, quanto maior o fluxo informacional gerenciado por uma determinada empresa, maior a sua vantagem econômica. Portanto, informações sobre hábitos dos cidadãos, afora outros dados pessoais, tornam-se a matéria-prima de uma economia redimensionada pelos avanços das TICs.

1.2.2.1 Você é a mercadoria

Considerando que os humanos pensam em forma de narrativa (Harari, 2018) e que a narração exerce uma seleção, só admitindo determinados acontecimentos (Han, 2016), variados autores têm tentado definir esta (nova) sociedade emaranhada por dados: sociedade da informação[24], sociedade de redes (Castells, 2002), vigilância de plataformas (Wood; Monaham, 2019), capitalismo de vigilância (Zuboff, 2021)e a economia do *big data*(O'Neil, 2017). Todavia, todos os autores convergem na constatação de que o custo para o tratamento, a coleta e armazenamento de dados é cada vez menor (Garcia, 2020) (*Vide Capítulo 1.2.1*).

Com a possibilidade de organizar dados de maneira mais escalável (*e.g., big data*), criou-se um mercado cuja base de sustentação é a sua extração e "comodificação" (Zuboff, 2015), ou seja, os dados são os insumos – o dado é o estado primitivo da informação, pois não é algo que *per se* acresce conhecimento (Bioni, 2021) – deste mercado: eles são os *inputs*[25] para

[23] No contexto do capitalismo informacional, como descrito por Dantas (1999), as grandes corporações atuam como centros de redes empresariais, coordenando um conjunto global de empresas interligadas. Essas corporações, como a Nike, utilizam tecnologias avançadas para analisar dados de mercado e vendas, identificando produtos ineficazes e ajustando suas estratégias de acordo com essas informações. O processo envolve a redistribuição dessas análises aos parceiros que integram suas redes globais, formando o que se denomina "corporações-redes", que se organizam por meio de rápidas redes de comunicação e processamento de informações.

[24] Segundo Sally Burch (2005), a expressão "sociedade da informação" consolidou-se na última década como o termo dominante. Isso ocorreu não necessariamente por uma clareza teórica, mas devido ao fato de ter sido adotada oficialmente nas políticas dos países mais desenvolvidos e promovida internacionalmente, especialmente com a realização de uma Cúpula Mundial dedicada ao tema.

[25] O *input* de dados refere-se à etapa inicial de inserção de dados em um sistema ou rede. Esse processo é fundamental para a criação de dados que, uma vez processados, geram informações que serão posteriormente analisadas.

que seja gerado determinado resultado (*outputs*[26])– predições comportamentais[27], comumente no formato de perfil daquele indivíduo. À vista disso, quanto mais dados são processados, maior a predictibilidade positivada, propiciando concomitantemente o aprimoramento do próprio modelo de processamento – sendo este um exemplo de *machine learning*[28].

Em suma, o que acontece é uma coleta de dados mais ampla do que seria necessária, alimentando o *machine learning*, sendo este, segundo Shoshana Zuboff (2021), o início da vigilância a partir do que ela convencionou chamar de *behavioralsurplus*[29]– ou superávit comportamental. Este produto (*output*) será vendido em mercados de comportamentos futuros, configurando uso secundário destes dados, pois distinto da finalidade originalmente aprovada.

Neste contexto em que se estrutura a economia baseada em dados (*data-driven economy*[30]) – na lógica do *machine learning* e do *big data* de acumular a maior quantidade possível de dados – é que a figura dos *data brokers*[31] emerge.

Em um instigante relatório de 2014, "*Data Brokers: A Call for Transparency and Accountability"* [32], a *Federal Trade Commission*[33] (FTC) teve a oportunidade de fazer um mapeamento da indústria de dados e do papel dos *data brokers*, empresas que coletam

---

[26] O *output* de dados refere-se à etapa final do processamento de informações, em que os dados previamente inseridos –*input* – e analisados são transformados em resultados concretos ou informações úteis. O *output* representa a saída dessas informações processadas, que podem ser utilizadas para tomar decisões estratégicas, otimizar operações e gerar valor para as empresas e indivíduos. Esse processo é essencial para a materialização dos benefícios derivados do processamento de dados, como a melhoria da eficiência, a redução de custos e a geração de *insights* que orientam ações futuras.

[27] O termo *predição comportamental* é frequentemente utilizado por Shoshana Zuboff em sua produção e se refere a estimativas baseadas na análise de dados que visam a antecipar ações e preferências de indivíduos ou grupos. Utilizando algoritmos e modelos estatísticos, essas predições permitem prever comportamentos futuros com base em padrões observados, sendo amplamente aplicadas em áreas como economia, *marketing* e gestão. Elas auxiliam na tomada de decisões estratégicas, na personalização de serviços e na otimização de processos, transformando dados em *insights* valiosos para a adaptação e melhoria das práticas organizacionais.

[28] Mohri, Rostamizadeh e Talwalkar (2018) definem aprendizado de máquina como um conjunto de métodos computacionais que utilizam a experiência para melhorar o desempenho ou para fazer previsões precisas.

[29] Zuboff (2021) descreve o capitalismo de vigilância como um sistema que, de forma unilateral, utiliza a experiência humana como matéria-prima gratuita para a conversão em dados comportamentais. Parte desses dados é usada para melhorar produtos e serviços, enquanto o restante é considerado superávit comportamental do proprietário, sendo direcionado para processos avançados de fabricação, como o "*machine learning*", para produzir previsões que antecipam as ações futuras de indivíduos.

[30] A *data-driven economy*, ou economia baseada em dados, é o valor social e econômico obtido através do compartilhamento de dados.

[31] De acordo com Frazão (2019), os *data brokers* são definidos como empresas que coletam informações pessoais dos consumidores e as revendem ou compartilham com outras empresas, operando como intermediários no mercado de dados pessoais e levantando preocupações sobre os riscos associados à privacidade e segurança dessas informações.

[32] FEDERAL TRADE COMMISSION. *Data Brokers. A Call for transparency and accountability.*Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-reportfederal-trade-commission-may-2014/140527databrokerreport.pdf>. Acesso em 09 de set. 2024.

[33] A *Federal Trade Commission* (FTC) é a Comissão Federal de Comércio dos Estados Unidos, um órgão que fiscaliza a segurança de dados corporativos e que atua em defesa dos interesses dos consumidores.

informações pessoais dos consumidores e as revendem ou compartilham com outras – também conhecidos como corretores de informações.

Ocupando um papel de destaque na *data-driven economy*, estas empresas não são de conhecimento dos consumidores gerais, visto que, não interagem diretamente com eles e, exatamente por este motivo, suas práticas e atividades permanecem desconhecidas. Por esta razão, o relatório buscou, a partir do mapeamento das práticas de nove *data brokers*, entender como esta indústria efetivamente funciona.

Em uma apertada síntese (Frazão, 2019), as principais conclusões do estudo foram:

> (i) os *data brokers* coletam informações sobre os consumidores de diversas e numerosas fontes comerciais, governamentais e públicas (incluindo nesta última mídias sociais, *blogs* e *internet*);
> (ii) os *data brokers* não usam apenas os dados crus (*raw data*) mas também os chamados dados derivados, que são as inferências já realizadas a partir dos dados crus;
> (iii) os *data brokers* combinam dados obtidos online e *offline* para atingirem os consumidores *online*;
> (iv) as principais utilizações comerciais dos dados são *marketing*, serviços de mitigação de riscos e serviços de busca de pessoas;
> (v) parte expressiva da coleta de dados ocorre sem o conhecimento dos consumidores;
> (vi) a indústria dos dados é complexa, com muitas camadas de *data brokers* que oferecem e trocam dados uns com os outros, sendo frequente o intercâmbio e a compra e venda de informações entre eles;
> (vii) os *data brokers* coletam e armazenam bilhões de dados que, na época da pesquisa, já cobriam praticamente todos os consumidores norte-americanos;
> (viii) qualquer que seja a metodologia utilizada, os *data brokers* coletam mais informações do que usam;
> (ix) uma das maiores aplicações dos dados é o desenvolvimento de modelos complexos para predizer o comportamento dos consumidores e para extrair inferências potencialmente sensíveis a respeito deles;
> (x) apesar dos benefícios da atividade de tratamento de dados, muitos dos propósitos pelos quais os *data brokers* coletam e usam dados apresentam riscos para os consumidores;
> (xi) as escolhas que os *data brokers* oferecem aos consumidores sobre os seus dados são amplamente invisíveis e incompletas, com grande ausência de transparência.

Ainda que tenha se passado mais de uma década da pesquisa, existem diversas evidências de que as práticas supramencionadas perduram e se intensificaram (Frazão, 2019).

Os *data brokers* não buscam justificar os supostos benefícios e vantagens que oferecem de forma "gratuita" ou acessível aos usuários. Ainda assim, o mercado de dados continua a se expandir, impulsionado por visões que consideram o modelo de negócios justo, pois os usuários receberiam compensações adequadas pelo fornecimento de seus dados, ou mesmo necessário,

sob o argumento de que existe um *trade-off*[34] entre inovação e privacidade[35]. Nesse contexto, a violação da privacidade seria vista como um mal necessário para o progresso tecnológico e os novos serviços que surgem dessa dinâmica.

1.2.3 Materializando conceitos

"As tecnologias mais profundas são aquelas que desaparecem no dia a dia, até se tornarem indistinguíveis da rotina" (WEISER, 1991, p. 94). Esse foi o diagnóstico feito por Mark Weiser em 1991, no conceito que ele denominou de "computação ubíqua"[36]. Décadas depois, sua previsão se concretizou. A interação homem-máquina tornou-se cada vez mais imperceptível, especialmente com o advento de dispositivos móveis como celulares e *tablets*. A portabilidade desses aparelhos permitiu que as pessoas permanecessem constantemente conectadas, com acesso à *internet* a qualquer momento e em qualquer lugar. Conforme uma pesquisa divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), em 2023, 88% dos brasileiros com 10 anos ou mais utilizavam a *internet*. Dentre esses usuários, 98,8% acessaram por meio de celulares[37], enquanto apenas 34,2% utilizavam microcomputadores domésticos, sendo essa proporção inferior aos 49,8% que acessaram a *internet* pela televisão (Nery, 2024).

Nesse contexto, em decorrência das mudanças tecnológicas recentes[38], seu uso não somente se tornou indistinguível da rotina, mas também criou uma relação de dependência dos cidadãos quanto às TICs, uma vez que, os serviços gratuitos de empresas como *Google*[39], *Facebook*[40], dentre outras, apelaram para as necessidades latentes desses indivíduos na busca de recursos para uma vida mais efetiva (Zuboff, 2021) em um ambiente institucional cada vez mais hostil. "Uma vez mordida, a maçã se tornou irresistível" (ZUBOFF, 2021, p. 409).

---

[34] O termo *trade-off* refere-se à situação em que é necessário fazer uma escolha entre opções mutuamente exclusivas, sob as quais ganhos em uma área implicam perdas em outra.

[35] Segundo Frazão (2019), a privacidade acaba sendo vista como um preço a ser pago ou um mal necessário para o avanço tecnológico e o surgimento de novos serviços, que se baseiam no uso intensivo de dados pessoais.

[36] Computação ubíqua é um conceito que descreve a integração profunda e constante da tecnologia no cotidiano das pessoas, de maneira quase invisível e onipresente.

[37] De acordo com dados do IBGE, em 2023, estimou-se que 163,8 milhões de brasileiros com 10 anos ou mais possuíam telefone móvel para uso pessoal, o que representava 87,6% da população nessa faixa etária (Nery, 2024).

[38] Segundo Liliane Paesani (2007), a sociedade atual vive uma revolução tecnológica sem precedentes, com a criação de um novo poder, o tecnológico, que encurta distâncias de tempo e espaço. Esse poder tem consequências significativas nas concepções sobre as relações entre território, política, economia e cultura, impactando regiões geográficas maiores e um número crescente de pessoas.

[39] Englobam-se nessa perspectiva as empresas vinculadas ao Google como: *Waze, Gmail, Youtube, Android etc.*

[40] Englobam-se nessa perspectiva as empresas vinculadas ao *Facebook* como: *Instagram, Whatsapp etc.*

Shoshana Zuboff (2021, p. 24), faz importantes reflexões sobre a dinâmica indivíduo-TIC, razão pela qual passamos a transcrever suas considerações:

> Os produtos e serviços do capitalismo de vigilância não são objeto de uma bolsa de valores. Não estabelecem reciprocidades construtivas produtor-consumidor. Em vez disso, são "ganchos" que seduzem usuários para suas operações extrativas nas quais nossas experiências pessoais são sucateadas e empacotadas como meios para fins de outros. Nós não somos os "clientes" do capitalismo de vigilância. Embora se diga que "se for de graça, então o produto é você", essa afirmativa também é incorreta. Nós somos as fontes do superávit crucial do capitalismo de vigilância: os objetos de uma operação de extração de matéria-prima tecnologicamente avançada e da qual é cada vez mais impossível escapar. Os verdadeiros clientes do capitalismo de vigilância são as empresas que negociam nos mercados de comportamento futuro.

Tradicionalmente no capitalismo, a relação entre consumidores e fornecedores é caracterizada pela troca direta de dinheiro por bens de consumo, formando um vínculo bilateral sob que o pagamento ocorre por meio de transferência pecuniária. Porém, na economia da informação, essa dinâmica se altera: os consumidores não pagam em dinheiro pelos produtos ou serviços, mas cedem seus dados pessoais em troca de publicidade direcionada. Isso configura uma relação plurilateral, pois envolve terceiros que financiam o processo com dinheiro. Nesse cenário, o consumidor acaba se tornando um produto, já que seus dados são parte essencial da operação econômica (Bioni, 2021).

1.2.3.1. Publicidade offline e publicidade online

O gerenciamento de informações pessoais dos consumidores é um elemento estratégico transformador do marketing em geral[41] (*Vide Capítulo 1.2.2*). É também um vetor de mutação da atividade publicitária como a tônica do que predomina nos modelos de negócios na *internet*.

A publicidade pode ser conceituada como qualquer forma paga de apresentação não pessoal e promoção de ideias, bens ou serviços por um patrocinador identificado (Kotler; Keller, 2012), a partir da qual se tem apenas informações a respeito das características do bem de consumo, como também, promove-se ao ato de consumo.

A publicidade tradicional pode ser caracterizada por métodos e canais que não envolvem a *internet*. Esse modelo utiliza mídias como televisão, rádio, impressos (jornais e revistas) e

[41] Segundo Kotler (2003), o *marketing* é tanto uma ciência quanto uma arte voltada para a exploração, criação e entrega de valor, com o objetivo de atender às necessidades de um mercado-alvo de forma lucrativa. Ele envolve a identificação de necessidades e desejos não atendidos, a medição do tamanho e do potencial lucrativo desse mercado e a segmentação, de modo a definir os produtos e serviços que melhor atendam ao público-alvo.

outdoors para alcançar um público amplo e influenciar as decisões de consumo por meio da exposição repetida a mensagens (Kotler; Keller, 2012).

A publicidade tradicional enfrentou no curso de sua história diversos desafios, incluindo a natureza unidirecional da comunicação, que limita o *feedback*[42] dos consumidores e restringe a capacidade de engajar em diálogo. Em consequência, a ciência mercadológica percebeu que a comunicação em massa era ineficiente visto que se desperdiçavam esforços com um público que não teria qualquer propensão a consumir o bem anunciado. Isso resulta em potencial desperdício de recursos, pois as mensagens nem sempre atingem o público-alvo de forma eficaz. Nesse contexto, buscando mitigar esses efeitos, surge a publicidade direcionada.

A publicidade direcionada envolve a entrega de anúncios a grupos específicos de consumidores, com base em dados demográficos, psicográficos e comportamentais – *input*. O *output* gerado – ao revelar predições comportamentais (*Vide Capítulo 1.2.2.1*) – permite que profissionais de *marketing* personalizem suas mensagens para alcançarem indivíduos que são mais propensos a responder positivamente, melhorando assim a eficiência e a eficácia de seus esforços publicitários – esse processo não necessariamente se dá exclusivamente no contexto *online*, visto que o processamento do *input* pode se dar também no contexto *offline*[43].

Nesse sentido, a ciência mercadológica percebeu que a *internet* – por meio de estratégias baseadas em dados – poderia propiciar uma abordagem publicitária mais efetiva. Ao utilizar plataformas *online*, mídias sociais e publicidade direcionada, as empresas podem se engajar em comunicação bidirecional com os consumidores, coletar *feedback* e medir com mais precisão a eficácia de suas campanhas. Essa abordagem melhora a eficiência do direcionamento, reduz o desperdício e promove um relacionamento mais interativo com o público (Kotler; Keller, 2012).

[42] O conceito de *feedback* pode ser definido como a comunicação feita entre duas ou mais pessoas, na qual uma delas é avaliada pelos demais com relação às suas ações, comportamentos, tarefas, entre outros.

[43] Embora haja uma ênfase crescente na digitalização e no acesso *online*, ainda existem formas relevantes de *input* de informações *off-line* que desempenham papel significativo na disseminação de conhecimento. Exemplos disso incluem a leitura de livros físicos, que permite a obtenção de conhecimento sem a necessidade de dispositivos eletrônicos ou conexão à *internet*; participação em palestras ou seminários presenciais, em que o conhecimento é transmitido diretamente por meio da comunicação verbal; consulta a enciclopédias e dicionários impressos; e interações em reuniões presenciais ou entrevistas, em que as informações são trocadas e registradas em formato analógico, como anotações em papel.

1.2.3.2 A vigilância na prática

Na prática, a abordagem publicitária de que se falou acima pode ser implementada por diversas ferramentas tecnológicas[44], das quais destacam-se os *cookies*[45](*Vide Capítulo 3.1.1.2*). Um *cookie* pode ser definido como um pequeno arquivo de texto armazenado pelo navegador (*web browser*), funcionando como uma "carteira de identidade" do usuário, permitindo a memorização dos dados e o reconhecimento de hábitos de navegação que podem ser transformados em informações relevantes tanto para o aprimoramento dos sites – *machine learning* – quanto para a oferta de anúncios publicitários, constituindo-se num polêmico mecanismo de vigilância.

Pelo registro de navegação dos usuários, é confeccionado um detalhado retrato de suas preferências (Nissenbaum; Barrocas, 2009), possibilitando a personalização de anúncios. Essa abordagem viabiliza a oferta de conteúdo publicitário diretamente relacionado aos interesses individuais de cada usuário. Nesse sentido, Bruno Ricardo Bioni (2021, p. 17), faz importantes ponderações no que se refere à vigilância gerada por meio dos cookies:

> Sabe-se o que ele (usuário) está lendo, quais os tipos de *websites* acessados, enfim, tudo aquilo em que a pessoa está efetivamente interessada e, em última análise, o que ela está mais suscetível a consumir com base nesse perfil comportamental. Quando o usuário navega na *internet*, há uma série de cliques (*clickstream*) que revela uma infinidade de informações sobre as suas predileções, possibilitando que a abordagem publicitária as utilize para estar precisamente harmonizada com elas.

O que implica na redução de custos da ação publicitária, uma vez que, o bem de consumo anunciado é relacionado especificamente aos interesses do consumidor, propiciando índices de indução ao consumo jamais alcançados pela publicidade *offline*. Mais que isso, os próprios cliques permitem mensurar a eficiência do anúncio publicitário.

"Os anunciantes trabalham olhando para trás, examinando seus êxitos passados, em vez de para frente, gerando ideias diretamente derivadas de resultados de estudos publicados" (Ávila; Bianchi, 2015). Igualmente, tanto as redes sociais quanto diversos outros serviços, revertem tal vigilância em um conhecimento para agregar eficiência à publicidade veiculada no

[44] São várias as técnicas de rastreamento do comportamento do usuário na *internet* para fins de reavaliar a autodeterminação informacional, dos quais são exemplos*: HTML5*, *flash cookies, evercookies etc.*

[45] Conforme Martins (2008), os programas de dados, conhecidos como fichários de dados, são utilizados principalmente para identificar o usuário, rastrear sua navegação e coletar informações úteis a seu respeito, especialmente com base em seus dados de navegação e consumo. Esses programas são geralmente enviados pelos provedores de *internet* aos navegadores dos usuários, ficando armazenados em diretórios específicos nos computadores.

ambiente virtual. Nesse sentido, a percepção de que os mesmos anúncios perseguem os usuários por diferentes *websites* (*remarketing*[46]) reflete uma ação coordenada entre diversos atores, entre os quais destacam-se as redes de publicidade (*ad networks*[47]), responsáveis por conectar milhares de aplicações, como *websites* que exibem (*publishers*) publicidade aos fornecedores, que querem anunciar (*advertisers*) um bem de consumo.

As redes de publicidade cooperam entre si (*ad exchanges*[48]), transacionando bases de dados para maximizar seu alcance e a precisão da segmentação de anúncios. Em vista disso, os *data brokers* (*Vide Capítulo 1.2.2.1*) desempenham um papel fundamental ao reunir dados de diversas fontes e comercializá-los, ou seja, operando como verdadeiros corretores de bancos de dados[49].

Por essa lógica, cada clique pode representar uma oportunidade de extração de valor, muitas vezes sem o pleno conhecimento do usuário sobre o alcance dessa vigilância. O uso "gratuito" dos serviços digitais (*zero-price advertisement business model*[50]) esconde uma transação implícita de dados pessoais (*trade-off)*, que levanta questões críticas sobre privacidade, segurança de dados e os limites éticos da coleta e uso dessas informações. A promessa de acesso sem custo monetário é, na verdade, um compromisso contínuo de cessão de dados, alimentando um ciclo econômico que transforma o consumidor em um produto altamente monetizável para o mercado publicitário (*Vide Capítulo 1.2.3*). Assim, estratégias de *marketing* digital não apenas otimizam a relação custo-benefício das campanhas, mas também desempenham um papel crucial na gestão da confiança e na mitigação dos riscos associados à privacidade dos consumidores.

---

[46] *Remarketing* significa fazer *marketing* novamente para a mesma pessoa. A intenção é gerar impacto mais de uma vez, sobre alguém que já demonstrou interesse no produto

[47] *Ad network* é uma organização que conecta anunciantes com um grupo de canais de mídia. Ela cumpre o papel de facilitar a compra e venda de inventário tornando desnecessária a negociação direta de um anunciante com muitos canais, facilitando os esforços dos dois lados da mesa. As *ad networks* podem incluir diferentes tipos de canais ou se focar em certos nichos (viagem, maternidade, etc.).

[48] *Ad exchange* é um sistema que possibilita a compra de mídia via leilão em tempo real. Ela conecta o anunciante diretamente aos canais ou a *ad networks* para veiculação de mídia. Em geral uma *ad exchange* possibilita acesso a um grande inventário de mídia, facilitando o processo de compra como um todo.

[49] Segundo Date (2003), um banco de dados pode ser descrito como uma coleção de dados operacionais logicamente relacionados, utilizados por uma organização para facilitar o gerenciamento e a manipulação das informações de maneira organizada e eficiente.

[50] A expressão é de Katherine J. Strandburg (2013).

1.2.3.3 A dependência é múltipla

À medida que a *internet* se torna parte integrante da vida cotidiana, os usuários cada vez mais se transformam em consumidores. Um exemplo claro dessa tendência é o crescimento acelerado do comércio eletrônico. No Brasil, o setor de *e-commerce* tem apresentado taxas de crescimento notáveis, alcançando um faturamento expressivo de R$185,7 bilhões em 2023 (ABCOMM, 2024).

Da mesma forma, à medida que a *internet* e o comércio eletrônico se consolidam como pilares essenciais do mercado global, o ambiente empresarial brasileiro tem experimentado transformações profundas. Empresas que ainda não adotaram uma presença digital robusta enfrentam desafios crescentes para se manterem competitivas. A ausência de estratégias de comércio eletrônico e *marketing* digital pode resultar em perda significativa de participação de mercado, à medida que consumidores se voltam preferencialmente para empresas que oferecem conveniência, variedade e personalização *online*.

Segundo dados da Associação Brasileira de Comércio Eletrônico (ABCOMM), em 2023, aproximadamente 87% dos consumidores brasileiros realizaram pelo menos uma compra *online* e a tendência é de crescimento contínuo desse percentual nos próximos anos (ABCOMM, 2024). As empresas que não se adaptam a essa realidade digital estão perdendo espaço: um estudo do Sebrae apontou que micro e pequenas empresas sem presença *online* registraram queda de 30% em seu faturamento durante o mesmo período (SEBRAE, 2023). Portanto, o cenário atual do mercado brasileiro evidencia a urgência da digitalização como fator crucial para a sobrevivência e expansão das empresas no país.

Nesse sentido, nota-se que não somente o cidadão se encontra em uma posição de dependência diante das TICs, mas os comerciantes também se veem pressionados a aderir a esse novo contexto econômico para garantir sua sobrevivência e competitividade no mercado. A crescente digitalização dos processos de compra e venda não apenas modifica os hábitos de consumo, mas também impõe uma reconfiguração das estratégias empresariais. Conforme destaca o professor e especialista em comércio eletrônico Alberto Luiz Albertin (2022, p. 01), da Fundação Getúlio Vargas (FGV): "A adoção das TICs deixou de ser uma vantagem competitiva para se tornar uma necessidade básica; empresas que não integram tecnologias digitais em suas operações e estratégias correm o risco de desaparecer do mercado".

Essa pressão é ainda mais acentuada em um cenário em que os consumidores esperam cada vez mais eficiência, disponibilidade de produtos e uma experiência de compra

simplificada, características que são possibilitadas pela utilização de plataformas digitais. Assim, a resistência à digitalização não é mais uma opção viável para os comerciantes, que devem se adaptar rapidamente para atender a essas novas demandas e assegurar sua posição no mercado.

1.3 A CIÊNCIA JURÍDICA E O CONSENTIMENTO NO CONTEXTO DA ECONOMIA DA INFORMAÇÃO

O entusiasmo excessivo dos usuários com os modelos de negócios da economia digital e os benefícios diretos que acreditam receber, aliado à dificuldade de entender plenamente seus impactos reais, impõe desafios adicionais aos reguladores (Frazão; Oliva; Tepedino, 2019). No contexto do capitalismo de vigilância, diante da assimetria informacional e dos aparentes benefícios trazidos pelas inovações, os reguladores frequentemente enfrentam um dilema: precisam encontrar um equilíbrio entre estimular o progresso tecnológico e garantir a proteção dos dados pessoais dos usuários (Barreto Junior; Naspolini, 2019) (*Vide Capítulo 2.1.3.2*). Historicamente, esse cenário contribuiu para que muitos negócios prosperassem em um ambiente de pouca regulamentação (*Vide Capítulo 3.1*), o que se mostrou conveniente para os principais *players* da indústria, permitindo-lhes operar com poucas restrições (Frazão; Oliva; Tepedino, 2019).

Este diagnóstico é fundamental, pois sem ele seria difícil avançar na compreensão do papel do consentimento na proteção dos dados pessoais, especialmente ao se confrontar com a passividade geralmente atribuída aos cidadãos em relação ao fluxo de suas informações pessoais.

1.3.1 Os riscos de uma nova era

Naturalmente tecnologias tão pervasivas (*Vide Capítulo 1.2.3.2*) não se envolvem na vida dos usuários sem apresentar qualquer ameaça. As inovações da "terceira era" (*Vide Capítulo 1.1*), trouxeram consigo riscos com elevados níveis de abstração e complexidade. Nesse sentido, sobrevém a ausência de conhecimento, de percepção, de previsibilidade e de controle no que concerne a situações fáticas que, criadas pelo momento da inovação, são experimentadas sem que haja uma efetiva consciência sobre o que se experimenta.

Portanto, à semelhança do que Baumann (2001) compreendeu quanto às relações humanas, pode-se dizer que há uma liquidez na relação ser humano/máquina e, sob essa perspectiva, se identifica o grande desafio a ser enfrentado nesse novo contexto socioeconômico: a proteção da personalidade do cidadão e de sua extensão — através de seus dados pessoais, os quais estão intimamente ligados à autonomia individual e à dignidade humana (*Vide Capítulo 2.1.1.2*) Os dados pessoais não são apenas uma representação de uma pessoa, mas uma verdadeira extensão da sua personalidade, como generalizado dos conceitos apresentados por Paul Schwartz (2000), em sua obra "*Internet privacy and thestate"*, reforçando a importância de tratá-los com o devido cuidado para assegurar a dignidade humana e a proteção individual em um ambiente digital em constante transformação.

Para além dos riscos à privacidade e ao controle sobre os dados pessoais, as TICs emergem como influenciadoras silenciosas do presente e do futuro dos cidadãos. Regularmente dados são processados por algoritmos que executam classificações e previsões potencialmente discriminatórias (*Vide Capítulo 2.1.2.1*), porque tendem a se basear em padrões históricos que podem refletir distorções e injustiças sociais[51]. Portanto, impactando diretamente a vida das pessoas, influenciando o acesso a crédito, empregos e serviços, o que se agrava com a possibilidade de os dados serem incompletos, desatualizados e incorretos, ou ainda, pela impossibilidade de sua retificação (Frazão, 2018).

1.3.2 Aprisionamento tecnológico e a autodeterminação informacional

Há uma nítida exposição. Dados são captados e utilizados para a personalização do usuário sem que ele conheça os processos e o universo em que está inserido. Não há como negar a assimetria da relação usuário-máquina tanto quanto à existência de riscos de natureza abstrata que decorrem desse vínculo.

> O capitalismo de vigilância age por meio de assimetrias nunca antes vistas referentes ao conhecimento e ao poder que dele resulta. Ele sabe tudo sobre nós, ao passo que suas operações são programadas para não serem conhecidas por nós. Elas acumulam vastos domínios de um conhecimento proveniente de nós, mas que não é para nós.(ZUBOFF, 2021, p. 26).

[51] Os dados pessoais sensíveis são aqueles associados às opções e características basilares da *persona* e, portanto, aptos a gerar situações de discriminação e desigualdade. Veja nesse sentido: MORAES, M. C. B. de (org.). Apresentação do autor e da obra. *In*: RODOTÀ, Stefano. *A vida na sociedade de vigilância:* A privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 1-12. Tradução: Danilo Doneda e Luciana Cabral Doneda.

Como resultado dos processos de vigilância da economia da informação, emerge o que Eli Pariser (2012) conceituou como *filter bubble* – também chamado de "bolha informacional". Em suma, a "bolha informacional" seria um estado de isolamento intelectual que surge como resultado de buscas personalizadas quando um algoritmo adivinha seletivamente quais informações um usuário gostaria de ver com base nas informações sobre o usuário, como localização, comportamento de cliques anteriores e histórico de pesquisas. Como resultado, os usuários ficam separados das informações que discordam de seus pontos de vista, isolando-os efetivamente em suas próprias bolhas culturais ou ideológicas.

O mencionado estado de isolamento intelectual, leva os usuários ao subsequente estado de aprisionamento tecnológico, que conforme explica a Lei de Metcalfe[52], é um estado no qual os usuários estão tão envolvidos com a tecnologia que, mesmo que um concorrente ofereça um serviço melhor, não vale a pena mudar.

> A lei diz que a utilidade de uma rede aumenta cada vez mais rápido sempre que acrescentamos uma nova pessoa à rede. Um aparelho de fax não tem muita utilidade se não conhecemos nenhuma outra pessoa que o possua, mas, se todos os nossos colegas de trabalho tiverem um fax, quem não fizer parte do grupo estará em grande desvantagem. O aprisionamento é o lado obscuro da lei de Metcalfe: o Facebook é útil, em grande medida, porque todos participam dele (PARISER, 2012, p. 34).

O aprisionamento tecnológico estrangula a capacidade do usuário de adaptação às mudanças do mercado, tornando-o dependente de um único fornecedor e à sua política de dados e, consequentemente, suprime qualquer capacidade de barganha.

A par disso, propõe-se a análise da autodeterminação – a autodeterminação é um princípio fundamental dos direitos humanos, que significa autonomia, auto responsabilidade, autorregulação e livre-arbítrio – informacional, um direito que se volta ao resguardo da pessoa na condição de usuário da *internet*, diante de qualquer potencial agressão que possa aviltar a sua esfera íntima ou privada. Nesse sentido, a autodeterminação informacional viria a resguardar a privacidade e a intimidade do usuário, assegurando que apenas as informações por ele autorizadas, e dentro dos limites por ele estabelecidos, poderiam ser utilizadas para esse fim.

---

[52] A Lei de Metcalfe é um princípio formulado por Robert Metcalfe, coinventor da *Ethernet,* que afirma que o valor de uma rede é proporcional ao quadrado do número de usuários conectados a ela. Em termos simples, à medida que mais pessoas se conectam a uma rede, como uma rede social ou de comunicação, o valor e a utilidade da rede aumentam exponencialmente.

Diante de todos esses riscos significativos e da necessidade de criação de mecanismos que protejam e deleguem ao usuário a capacidade de autodeterminação informacional, emerge a necessidade de controle na coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, armazenamento e eliminação de dados pessoais[53], o que se busca no Brasil por meio da Lei n° 13.709/2018 - Lei Geral de Proteção de Dados –, ou simplesmente LGPD.

[53] Tratamento de dados nos termos do Art. 5º, da Lei n° 13.709/2018, consiste em "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"

CAPÍTULO 2 - DADOS PESSOAIS: DIREITO DA PERSONALIDADE E PROTEÇÃO PARA ALÉM DA AUTODETERMINAÇÃO INFORMATIVA

2.1 DADOS PESSOAIS COMO UM DIREITO DA PERSONALIDADE

Os direitos da personalidade, focados na proteção dos aspectos fundamentais da pessoa humana, adquirem nova relevância com o avanço digital e o tratamento de dados pessoais. Esses dados, que refletem e projetam a identidade de cada indivíduo no ambiente digital, ampliam o entendimento jurídico da personalidade, demandando uma abordagem normativa que contemple as transformações tecnológicas e seus impactos sobre a dignidade da pessoa humana e a autodeterminação informativa.

2.1.1 Personalidade e direitos da personalidade

O termo “personalidade” – do latim *personalitate* – é definido como “qualidade pessoal". Caráter essencial e exclusivo de uma pessoa", sendo caracterizado como a totalidade dos atributos que tornam um indivíduo único e distinto dos demais (Dicionário Brasileiro da Língua Portuguesa, 1987, p. 1321). “No sentido jurídico, é a aptidão que tem todo ser humano, por força da lei, de exercer direitos e contrair obrigações” (GUIMARÃES, 1995, p. 437).

No que concerne os direitos da personalidade, deve-se considerar a personalidade como um bem jurídico[54], que por sua vez, configura um valor cultural de cunho axiológico[55]. Neste sentido, o ordenamento jurídico não cria o bem jurídico, apenas o encontra, pois o fim do Direito é proteger os interesses do ser humano e estes preexistem à intervenção normativa. Com efeito,

[54] Segundo Norberto Bobbio (1995, p. 45), bem jurídico é "o interesse tutelado pela norma jurídica, que constitui o objeto de proteção do direito". Trata-se de um valor ou interesse que o ordenamento jurídico reconhece como digno de proteção, buscando assegurar o desenvolvimento harmônico da sociedade e garantir direitos essenciais aos indivíduos.

[55] Um “valor cultural de cunho axiológico” refere-se a um princípio ou bem que é considerado valioso pela sociedade com base em critérios éticos, morais e culturais. Axiologia, o estudo dos valores, indica que esses bens não podem ser mensurados ou quantificados de forma direta. Segundo Miguel Reale (2002), a ideia de atribuir números ou medidas a elementos axiológicos é incompatível com sua natureza, pois os valores não possuem uma dimensão que permita sua mensuração, embora em certas situações práticas, como na valoração de bens materiais, seja possível estabelecer parâmetros de preço por razões pragmáticas. Alexandre Martins (2008) complementa esse entendimento ao afirmar que essa quantificação tem como propósito facilitar o cotidiano, sem, contudo, refletir o valor intrínseco e real desses bens, que permanecem imensuráveis em sua essência. No caso da personalidade, trata-se de um valor cultural que, por sua importância e ligação com a dignidade humana, transcende qualquer forma de mensuração, sendo reconhecido pelo ordenamento jurídico como um bem fundamental e pré-existente.

no sentido jurídico, a personalidade é um bem, aliás, o primeiro pertencente à pessoa. Neste sentido, aduz Elimar Szaniawski (2002, 35):

> Personalidade se resume no conjunto de caracteres do próprio indivíduo; consiste na parte intrínseca da pessoa humana. Trata-se de um bem, no sentido jurídico, sendo o primeiro bem pertencente à pessoa, sua primeira utilidade. Através da personalidade, a pessoa poderá adquirir e defender os demais bens (...). Os bens que aqui nos interessam são aqueles inerentes à pessoa humana, a saber: a vida, a liberdade e a honra, entre outros. A proteção que se dá a esses bens primeiros do indivíduo denomina-se direitos da personalidade.

A partir da análise de Szaniawski, entende-se que a personalidade, como bem jurídico, é essencial para a proteção dos direitos fundamentais de cada indivíduo, indo além de uma visão meramente patrimonialista ao abarcar dimensões morais e existenciais. Esse entendimento encontra suas raízes no desenvolvimento histórico dos direitos da personalidade, especialmente a partir do jusnaturalismo, que enfatiza a dignidade humana e os direitos inatos decorrentes da própria natureza do ser humano. A evolução do pensamento jurídico, particularmente com o jusracionalismo, consolidou a proteção desses direitos ao focar na razão e na dignidade como pilares centrais, influenciando a forma como os direitos da personalidade passaram a ser tratados nas codificações jurídicas e na construção do sistema de proteção vigente, como será abordado a seguir.

2.1.1.1 A travessia dos direitos da personalidade

Pode-se dizer que o prefácio da construção normativa dos direitos da personalidade se dá no direito grego (*hybris*[56]) e no direito romano (*actioin iuriarum*[57]). Diferentemente de outras culturas jurídico-legais anteriores (*e.g.,* Código de Hamurabi) que baseavam a tutela da pessoa humana tão somente na tutela da integridade física, passou-se a situá-los também no campo moral (*e.g*., tutela da honra[58]) (Bioni, 2021).

---

[56] De acordo com Rabindranath Capelo de Sousa (1995), o pensamento filosófico grego desempenhou um papel crucial na formação da teoria dos direitos da personalidade, destacando o dualismo entre o direito natural, visto como uma ordem superior originada da natureza, e o direito positivo, composto pelas leis humanas. Nesse contexto, o homem passou a ser compreendido como a fonte e o propósito tanto da lei quanto do direito, o que trouxe um novo significado às questões relacionadas à personalidade, à capacidade jurídica individual e aos direitos da personalidade de cada pessoa.

[57] Em Roma, a proteção jurídica era dada à pessoa, no que concerne a aspectos fundamentais da personalidade, como a *actioin iuriarum*, que era dada à vítima de delitos de iniuria, que poderia ser a agressão física, como também, a difamação, a injúria, e a violação de domicílio (AMARAL, 2008).

[58] Veja nesse sentido: GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. Novo curso de Direito Civil, v. 3: Responsabilidade Civil. 17. ed. São Paulo: Saraiva Educação, 2019.

Essa orientação de uma ciência jurídica focada na pessoa vem a encontrar sinergia no jusnaturalismo, especialmente a partir da concepção empregada por Hugo Grócio (1625)[59] no século XVII. Enquanto as fases anteriores do jusnaturalismo – antigo e medieval[60] –, entendem a existência de um direito natural inato como algo vinculado à uma divindade ou ao cosmo, o jusnaturalismo racional–jusracionalismo[61]– de Grócio propõe a existência de um direito inato ditado pela razão, decorrente da própria natureza humana. Nesse sentido aduz Franz Wieacker (2004, p. 340):

> Contudo, a partir do próprio Grócio não existia ainda nenhuma via direta para a renovação metodológica da sistemática da ciência jurídica positiva no espírito do jusnaturalismo. As novas intenções do seu direito das gentes já tinham, por certo, estourado com muitas das convenções da teologia moral e da filosofia escolástica. Mas a relação desta nova ética com as disciplinas tradicionais não tinha ainda sido definida de novo e os próprios princípios do direito natural não tinham ainda sido ordenados num sistema de premissas e conclusões não contraditórias. Foram estas as duas tarefas realizadas pela segunda fase, matemática e sistemática, do jusracionalismo, baseada no método naturalista e gnosiológico de Galileu e Descartes.

A partir da fase sistemática, pode-se falar de forma efetiva sobre o juspositivismo, que, embora influenciado pelo cientificismo da modernidade, se fundamenta em bases antropológicas. Essa corrente não apenas busca o rigor metodológico e a sistematização das normas, mas também compreende o direito como uma construção derivada das relações humanas e da experiência social. Nesse contexto, a teoria jurídica europeia, que até então focava na exegese e na interpretação de textos específicos, adquire uma dimensão lógica e demonstrativa, desenvolvendo-se como um sistema fechado (Ferraz Júnior, 2003) com traços metodológico-sistemáticos. Tal racionalidade buscava aproximar a ciência jurídica da matemática, priorizando valores como previsibilidade, certeza e segurança jurídica, ainda que, por vezes, em detrimento da justiça efetiva.

Com isso, inaugura-se a era das codificações, marcada pelo domínio da legislação nos sistemas jurídicos. Nesse ambiente transformador do jusnaturalismo, emergem no direito

---

[59] Hugo Grócio (*Huig de Groot*), enunciado no *de iure belli a pacis de 1625*.

[60] Segundo Norberto Bobbio (2004), o jusnaturalismo pode ser analisado a partir de três contextos jurídico-políticos distintos. O Jusnaturalismo antigo, de caráter cosmológico, entende o direito natural como uma lei intrinsecamente ligada à natureza, quase instintiva para todos os seres animados. O jusnaturalismo medieval, de caráter teológico, considera o direito natural como uma lei criada pela divindade e revelada aos homens. Já o jusnaturalismo moderno, de caráter racional, interpreta o direito natural como uma lei fundamentada na razão, sendo específica do homem, que a descobre de forma autônoma em si mesmo.

[61] Conforme aponta Wieacker (2004), o jusracionalismo constitui apenas uma etapa limitada no contexto mais amplo e histórico das diversas expressões do jusnaturalismo.

privado as noções de negócio jurídico, relação jurídica e declaração de vontade, abstrações influenciadas pelo *pandectismo*[62] que derivam desse movimento racionalista.

> Porque onde não há república, conforme já se mostrou, há uma guerra perpétua de cada homem contra o seu semelhante, na qual portanto cada coisa é de quem a apanha e conserva pela força, o que não é propriedade nem comunidade, mas incerteza. Isso é a tal ponto evidente que até Cicero (um apaixonado defensor da liberdade), numa arenga pública, atribui toda propriedade às leis civis: Se as leis civis, disse ele, alguma vez forem abandonadas, ou negligentemente conservadas (para não dizer oprimidas), não haverá nada mais que alguém possa estar certo de receber dos seus antepassados, ou deixar aos seus filhos. E também: Suprime as leis civis, e ninguém mais saberá o que é seu e o que é dos outros. Visto, portanto, que a introdução da propriedade é um efeito da república, que nada pode fazer a não ser por intermédio da pessoa que a representa, tal propriedade só pode ser um ato do soberano, e consiste em leis que só podem ser feitas por quem tiver o poder soberano. Bem o sabiam os antigos, que chamavam *NÓJ.lOÇ* (quer dizer, distribuição) ao que chamamos lei, e definiam a justiça como a distribuição a cada um do que é seu. (HOBBES, 2003, p. 211)

As ponderações de Thommas Hobbes[63] (2003) antecipam as transformações de cunho patrimonialista que acometem as codificações civis que seguiram após o contexto jusracionalista do século XVIII. A excessiva carga patrimonialista decorre, justamente, das abstrações *pandectistas* mencionadas anteriormente, tais quais, declaração de vontade, relação e negócio jurídico. Nesse sentido, a ciência jurídica acabou por se distanciar de uma visão antropocêntrica e extrapatrimonial. Por este motivo, os direitos da personalidade não adquiriram a importância que lhes seria devido no direito privado naquele contexto, ainda que tenham sido desenhados e sistematizados anteriormente (Villey, 2005).

A tutela dos direitos da personalidade tampouco encontrou terreno fértil no período que se sucedeu do pós-iluminismo ao fim da Segunda Guerra (1945)[64]. A escravidão e os regimes nazifascistas, esfacelaram, todos eles com a chancela da ciência jurídica (juspositivismo), a ideia da prometida universalidade de direitos do "homem" proposta pelo jusnaturalismo[65] (Bioni, 2021).

---

[62] O *pandectismo*, escola jurídica alemã do século XIX, dedicou-se a sistematizar o Direito Romano, buscando construir um sistema jurídico estruturado de forma lógica e racional. Suas abstrações permitiram o desenvolvimento de conceitos gerais, como "obrigação" e "direito subjetivo," que facilitavam a aplicação das normas a casos concretos. Esse enfoque tornou o direito mais flexível e universal, reduzindo a necessidade de legislações detalhadas para cada situação específica e promovendo uma interpretação mais ampla e adaptável das normas jurídicas.

[63] Para Michel Villey (2005), a contribuição original de Hobbes consistiu em sua capacidade de construir uma estrutura que gera soluções jurídicas com base na natureza, mas sem deduzi-las diretamente.

[64] Ainda que as primeiras manifestações dos direitos da personalidade nas legislações dos povos chamados de "cultos", ou seja, sediados pretensamente na Europa, datem do século XIX, essas ocorreram de maneira fragmentada e bastante incompleta (De Souza, 2006).

[65] Norberto Bobbio (2004) aponta que o jusnaturalismo, ao propor uma teoria de direito absoluto e universalmente válido fundamentado na razão, fornecia bases doutrinárias para uma reforma racional da legislação.

Os traumas enfrentados no pós-guerra levaram à proliferação do princípio da dignidade humana nas constituições (Zanini, 2011), enquanto a própria Declaração Universal de Direitos Humanos das Nações Unidas[66] deu o passo determinante em direção a proteção dos direitos existenciais da pessoa humana. É no âmbito do direito privado, especialmente na Alemanha, que se inicia o desenvolvimento doutrinário dos direitos da personalidade, a partir da análise de decisões jurisdicionais em casos concretos, apreciados por juristas que passaram a reconhecer a existência de uma nova categoria de direitos merecedores de especial proteção.

Karl Larenz, célebre jurista alemão, destaca que:

> Na Alemanha, a sensibilidade, depois da guerra, em face de toda sorte de menosprezo à dignidade humana e desapreço à personalidade por parte do Estado e a multiplicação dos atentados a esta por particulares em razão dos progressos da técnica moderna, incentivaram os tribunais a reconhecer, com fundamento em artigos da Constituição, o denominado direito geral da personalidade, isto é, o direito da pessoa humana a ser respeitada e protegida em todas as suas manifestações imediatas dignas de tutela jurídica, assim como na sua esfera privada e íntima (*Apud* GOMES, 1983, p. 251-252).

Desse contexto, provém a "despatrimonialização" do direito civil. Isto é, o ser humano torna-se o foco da tutela jurídica.

A Constituição Federal da Alemanha (1949) incorporou, ao lado do princípio da dignidade humana, o direito ao livre desenvolvimento da personalidade[67], reforçando a proteção aos direitos individuais. De forma semelhante, o Pacto Internacional de Direitos Civis e Políticos de 1966 estabeleceu diretrizes específicas para os direitos da personalidade no âmbito privado, criando um padrão internacional de proteção[68]. Assim, diante da multiplicidade de influências e do fortalecimento das concepções sobre a importância dos direitos da personalidade, esses direitos passaram a ser replicados em diversas codificações privadas ao redor do mundo, ampliando sua abrangência e aplicação jurídica.

No ordenamento jurídico brasileiro, somente em 1988, com a promulgação da Constituição vigente é que se erigiu um sistema constitucional consentâneo com a pauta

---

[66] Este texto elenca como direitos da personalidade: o direito à igualdade, à liberdade, à segurança e à propriedade.
[67] A Lei Fundamental da República da Alemanha (1949) prevê em seu artigo 2°: "Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral."
[68] O Pacto Internacional de Direitos Civis e Políticos de 1966, adotado pela ONU, estabelece normas vinculantes para a proteção dos direitos civis e políticos fundamentais, impondo aos Estados signatários a obrigação de assegurar esses direitos. Ele promove a padronização internacional da proteção aos direitos da personalidade, incluindo liberdades essenciais como a de expressão, associação e o direito à vida.

valorativa afeta à proteção do ser humano em suas mais vastas dimensões, em tom nitidamente principiológico, a partir do reconhecimento de sua dignidade intrínseca[69].

A Carta Magna brasileira arrolou os direitos fundamentais em seu título II (arts. 5° a 17); precedido pelo título I (arts. 1° a 4°), que se dedica aos princípios fundamentais. Esses dispositivos por integrarem a CF/1988, constituem normas orientadoras de todo o sistema.

Veja nesse sentido o art. 5º, X da CF: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Além da mencionada proteção constitucional, o Código Civil (CC) de 2002 (arts. 11 a 21) passou a tutelar "infraconstitucionalmente", no âmbito do direito privado, os direitos da personalidade. Essa positivação, todavia, é bastante recente e fruto de uma evolução paulatina.

A Lei do Ventre Livre (1871) e a Lei dos Sexagenários (1885) podem ser citadas como percursoras dentre as normas expressas a tutelarem direitos da personalidade, ao "limitarem" a escravidão, reconhecendo um direito básico do ser humano: o direito à liberdade, "efetivamente" concretizado pela Lei Áurea (1988). É a fase embrionária da positivação dos direitos da personalidade no Brasil.

No CC de 1916, a doutrina brasileira já reconhecia os direitos da personalidade de forma implícita, mediante a interpretação de dispositivos que versavam remotamente sobre os aspectos extrapatrimoniais das relações sociais[70].

A matéria só ganhou ares de sistematização a partir do anteprojeto do CC de 1963, elaborado por Orlando Gomes. Diante da generalidade dos ordenamentos jurídicos das nações europeias, o projeto enumerou os direitos da personalidade como, por exemplo: o direito ao nome, à imagem, à liberdade, à honra, à integridade física e, por fim, os direitos autorais. Esse movimento representou uma ruptura com a perspectiva individualista e patrimonialista presente no CC de 1916, cujas bases estavam fortemente influenciadas pelo CC francês.

---

[69] A Constituição Federal de 1988 adota a dignidade da pessoa humana como princípio central, refletindo a concepção kantiana de valor intrínseco do ser humano, fundamentada na autonomia e racionalidade. Em Kant (2008), o direito limita a liberdade individual para garantir uma ordem pública justa, o que, no contexto brasileiro, se traduz na ampla proteção dos direitos fundamentais, promovendo um Estado Democrático de Direito orientado pela dignidade, liberdade e igualdade.

[70] Antônio Carlos Morato (2012) destaca que o CC de 1916 já abordava diversos direitos da personalidade, incluindo o direito à vida, à integridade física, à honra e à liberdade, a partir do artigo 1.537. Esses artigos previam o direito à indenização em casos de homicídio, lesão física, injúria, calúnia e ofensa à liberdade pessoal, detalhando compensações específicas conforme o tipo de dano sofrido, o que evidencia uma proteção parcial e fragmentada desses direitos na legislação da época.

Após décadas de elaboração e tramitação nas casas legislativas, um novo CC brasileiro foi aprovado e publicado por meio da Lei nº 10.406, de 10 de janeiro de 2002, e trouxe consigo muitas das ideias que Orlando Gomes idealizou no passado ao dedicar um capítulo próprio aos direitos da personalidade, contendo 11 artigos que elencam expressamente: o direito ao corpo (arts. 13 a 15); o direito ao nome e ao pseudônimo (arts. 16 a 19); direito autoral, à imagem, à honra, à boa fama (art. 20). Em que pese esta tipificação, os direitos da personalidade não se restringem a estes previstos pelo legislador; não se está diante de um rol taxativo[71].

Atualmente, é amplamente reconhecido que a dogmática tradicional não consegue resolver todos os problemas jurídicos das sociedades contemporâneas[72]. Em resposta a essa complexidade, a cláusula geral se destaca como a técnica mais adequada, já que as normas tradicionais, isoladamente, não conseguem regular completamente a vida social. Wambier (2005, p. 60) explica essa técnica:

> Cláusulas gerais são normas que explicitam princípios jurídicos e têm por função permitir ao Código Civil abranger hipóteses criadas pela contínua evolução social, que exigem disciplina. Assim, as cláusulas gerais têm um potencial de abrangência muito maior do que as regras tradicionais, que trazem em si suas próprias hipóteses de incidência.

A abordagem aberta das cláusulas gerais é essencial para evitar que os direitos da personalidade se tornem rígidos e incapazes de garantir uma tutela efetiva. Dada a importância desses direitos, a adoção de uma cláusula geral para sua proteção eliminaria a necessidade de listar exaustivamente suas espécies e características, permitindo o reconhecimento de novos direitos à medida que surgissem. Assim como os princípios jurídicos, as cláusulas gerais utilizam uma linguagem aberta, com conceitos vagos ou indeterminados, o que não representa um defeito de linguagem, mas uma característica adequada à realidade contemporânea, marcada pela instabilidade e pela rápida transformação social impulsionada pelas TICs no contexto da "sociedade da informação".

---

[71] Dispersos ao longo do diploma existem outros dispositivos relativos à responsabilidade derivada da violação de direitos da personalidade, como é o caso do homicídio (art. 948), dos ferimentos e outras ofensas à saúde (arts. 949 e 950), da injúria, difamação e calúnia (art. 955) e das ofensas à liberdade pessoal (art. 954).

[72] Segundo Rabindranath Capelo de Sousa (1995), a tutela fragmentada das diversas expressões da personalidade sujeita o indivíduo ao controle estatal. Ele defende que a unidade e expansão da personalidade humana e a centralidade do indivíduo nas normas jurídicas são fundamentais para a consagração de um direito geral da personalidade, que serviria como matriz e complemento dos direitos específicos da personalidade. Assim, a proposta não é apenas ampliar esses direitos específicos, mas estabelecer um direito geral da personalidade com um objeto claro e delimitado.

No ordenamento jurídico brasileiro, observa-se a opção pelo léxico *expansionista*[73] no preâmbulo da CF e da LGPD. Paralelamente, existe também uma proteção *reducionista*, prevista tanto no CC brasileiro quanto em leis esparsas[74].

2.1.1.2 Dados pessoais como projeção de uma nova identidade

Com base na definição semântica de personalidade (*Vide Capítulo 2.1.1*), os direitos da personalidade podem ser conceituados como um conjunto de características inerentes a um sujeito, que conformam a projeção da pessoa humana (Carvalho, 2012). Nome, honra, imagem, integridade física e psíquica seriam apenas alguns dentre uma série de outros atributos que dão forma a esse prolongamento[75]. Gustavo Tepedino (2008, p. 29) esclarece o conceito ao afirmar:

> Tem-se personalidade como conjunto de características e atributos da pessoa humana, considera-se como objeto de proteção por parte do ordenamento jurídico. A pessoa, vista deste angulo, há de ser tutelada das agressões que afetam a sua personalidade. (...) Dito diversamente, considerada como sujeito de direito, a personalidade não pode ser dele o seu objeto. Considerada, ao revés, como valor, tendo em conta o conjunto de atributos inerentes e indispensáveis ao ser humano (que se irradiam da personalidade), constituem bens jurídicos em si mesmos, dignos de tutela privilegiada.

Os avanços tecnológicos recentes e a crescente digitalização das relações humanas (*Vide Capítulo 1.2.1*), impõem uma reinterpretação das formas pelas quais a personalidade se manifesta e se projeta. No contexto do *big data*, os dados pessoais emergem como o veículo central de projeção da personalidade no ambiente digital, representando, de maneira simbólica e real, fragmentos da identidade individual. Em vista disso, a personalidade já não pode ser concebida de maneira isolada do contexto informacional no qual o sujeito está inserido.

Portanto, os dados pessoais são "expressões diretas da individualidade" e seu tratamento repercute o indivíduo nas esferas sociais e jurídicas. Essa relação íntima entre dados pessoais e personalidade evidencia como as novas tecnologias demandam uma expansão do conceito

[73] Bruno Ricardo Bioni (2021) argumenta que o conceito de dados pessoais é fundamental para o aperfeiçoamento da normatização, pois define os limites da própria proteção jurídica. Ele conclui que o vocabulário utilizado para essa definição opera como um filtro que pode restringir (reducionista) ou expandir (expansionista) a moldura normativa de uma lei de proteção de dados pessoais, influenciando a amplitude dessa tutela.

[74] Um exemplo é o art. 223-C da CLT, com a redação dada pela Lei nº 13.467/2017: "A honra, a imagem, a intimidade, a liberdade de ação, a autoestima, a sexualidade, a saúde, o lazer e a integridade física são os bens juridicamente tutelados inerentes à pessoa física."

[75] Esses são, por exemplo, algumas das espécies de direitos da personalidade listadas pelo CC (*Vide Capítulo 2.1.1.1*).

tradicional de personalidade (*e.g.,* cláusula geral), para incluir as várias formas de representação do indivíduo no ciberespaço. Em vista disso, Adriano de Cupis (2008, p. 180) infere:

> O indivíduo como unidade da vida social e jurídica, tem necessidade de afirmar a própria individualidade, distinguindo-se dos outros indivíduos, e, por consequência, ser conhecido por quem é na realidade. O bem que satisfaz essa necessidade é o da identidade, o qual consiste, precisamente no distinguir-se das outras pessoas nas relações sociais.

Nesse sentido, os dados pessoais, segundo o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, são definidos como, qualquer informação relativa a uma pessoa física identificada ou identificável.

No Brasil, a LGPD adota uma conceituação similar, reconhecendo que os dados pessoais não são apenas um conjunto de informações descontextualizadas, mas refletem e projetam facetas da identidade pessoal, social e jurídica do indivíduo. Conforme ensina Celso Lafer (2005, p. 133), "a personalidade jurídica deve ser protegida de qualquer tipo de invasão que possa vulnerar a dignidade da pessoa humana".

No contexto atual de intensa digitalização e avanços tecnológicos, a relação entre dados pessoais e personalidade tornou-se ainda mais intrincada. Dados pessoais agora funcionam como veículos centrais de projeção da personalidade no ambiente digital, representando fragmentos simbólicos e reais da identidade individual (Rodotà, 2012). Esse cenário impõe uma reinterpretação do conceito tradicional de personalidade, exigindo que se considere a projeção do indivíduo no ciberespaço como parte integrante da sua identidade (Rodotà, 2012).

O contexto socioeconômico atual se orienta e se movimenta a partir de "signos identificadores" dos cidadãos (*Vide Capítulo 1.2.3.2*). Portanto, é crucial que esses "dossiês digitais" reflitam informações precisas, de modo a projetar dignamente a identidade do titular dessas informações.

Além disso, Stefano Rodotà (2008), que trata do direito à privacidade e à proteção de dados, argumenta que a proteção desses dados não é apenas uma questão de privacidade, mas de proteção integral da dignidade humana, uma vez que o tratamento inadequado dessas informações pode gerar danos irreversíveis à integridade pessoal (*Vide Capítulo 1.3.1*) e até mesmo à coletividade[76].

[76] Stefano Rodotà (2008) alerta que o manejo inadequado de dados na "sociedade da informação" pode gerar condições propícias para práticas autoritárias, sem os sinais repressivos tradicionais, como prisões ou torturas em massa, que usualmente acompanham regimes totalitários. Ele destaca a necessidade de uma revisão dos valores fundamentais para garantir que liberdade e democracia possam se expandir plenamente. Nesse contexto, não basta

Em síntese, os dados pessoais não são apenas um reflexo de aspectos objetivos de um indivíduo, mas representam uma parte crucial de sua personalidade, identidade e dignidade. A proteção desses dados é uma questão essencial para a garantia dos direitos fundamentais e da própria integridade do sujeito no mundo contemporâneo.

2.1.2 Personalidade em evolução: dados sensíveis e IoT

Miguel Reale (2005) sustenta que nenhum conteúdo existencial pode existir como ato isolado, uma vez que a identidade está inextricavelmente ligada à "condicionalidade corpórea social do eu" indicando que a subjetividade só se torna real em um contexto de intersubjetividade ou sociedade, em que as identidades são determinadas e legitimadas coletivamente. Em consonância com esse entendimento, George Herbert Mead (1934) também argumenta que a identidade e a personalidade são construídas a partir das interações sociais. Através de sua teoria do "interacionismo simbólico"[77], Mead enfatiza que a compreensão de si – ou *self*– emerge das relações sociais e da troca de símbolos e significados, ressaltando o caráter relacional da construção da identidade.

O psicólogo Albert Bandura (1977) complementa essa visão ao destacar a importância do aprendizado social na formação da personalidade. Através da observação de comportamentos e das interações sociais, os indivíduos internalizam normas e valores que moldam suas ações e pensamentos. O fluxo informativo, neste sentido, é mediado por modelos sociais que servem de referência para a construção da autoimagem e das relações interpessoais. No contexto da *data-driven economy*, esses modelos são amplamente influenciados pelos dados pessoais que os indivíduos compartilham *online*, criando uma projeção pública da identidade que pode influenciar a percepção de si mesmos e dos outros.

As TICs ampliaram significativamente o alcance e a velocidade do fluxo informativo. As redes sociais, especialmente, desempenham um papel crucial ao facilitar a troca de informações pessoais e permitir a construção de identidades múltiplas e dinâmicas. Nesse sentido, Bruno Ricardo Bioni (2021, p. 83) argumenta:

---

apenas a tutela de direitos individuais, mas torna-se essencial fortalecer a percepção coletiva e aprimorar os mecanismos institucionais de resposta, visando a proteger a sociedade contra a escalada de vigilância e controle autoritário.

[77] Casagrande (2016) aponta que, para Mead, a vida se organiza e se desenvolve sobre um fundamento social, sendo o *self* estruturado simbolicamente. Esse entendimento envolve três premissas fundamentais: o reconhecimento do caráter intersubjetivo e social da vida humana e a primazia da sociedade sobre o indivíduo; a indissociabilidade entre sujeito e sociedade; e a centralidade da comunicação simbólica na formação do *self* e na evolução da comunidade humana.

> O ser humano não é uma ilha, ele se conforma e se desenvolve quando se relaciona com os demais 'no seio da sociedade que o abriga. Nesse sentido, os dados pessoais, não só se caracterizam como um prolongamento da pessoa (subjetividade), mas, também, influenciam essa perspectiva relacional da pessoa (intersubjetividade).

Diante dessa realidade, é crucial discutir a importância da tutela jurídica dos dados pessoais na dimensão relacional do indivíduo. A proteção desses dados é essencial para garantir que o cidadão não seja discriminado e que sua liberdade não seja comprometida.

2.1.2.1 Dados sensíveis: o direito a isonomia e não discriminação

Bruno Ricardo Bioni (2021) define dados sensíveis como sendo uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação.

Nessa perspectiva, os dados pessoais sensíveis são aqueles que estão associados a opções e características fundamentais da pessoa e, portanto, têm o potencial de gerar situações de discriminação e desigualdade. É com base na possibilidade de uso discriminatório, tanto pelo mercado quanto pelo Estado, que os dados sensíveis se relacionam a contextos nos quais podem ocorrer violações de direitos devido à sua natureza. Portanto, tal tutela jurídica busca garantir a ausência de traços diferenciais nas relações sociais, a fim de possibilitar que o indivíduo desenvolva livremente sua personalidade (Bioni, 2021).

Além dos dados que derivam da constituição biológica da pessoa, como raça e etnia, a natureza sensível de um dado pode também resultar de sua associação direta com a autodeterminação individual, como no caso de convicções políticas, religiosas, filosóficas, filiação sindical, orientação sexual, entre outros[78]. Esses aspectos da personalidade tornam o indivíduo especialmente vulnerável a distinções ou discriminações, pois são dados pessoais suscetíveis de uso para fins discriminatórios, como estigmatização, exclusão ou segregação. O tratamento inadequado desses dados compromete a dignidade do titular, afetando sua identidade pessoal e privacidade (Frazão; Oliva; Tepedino, 2020).

[78] O artigo 5º, inciso II, da LGPD elenca os dados pessoais considerados sensíveis, definindo-os como aqueles relacionados à 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.

Não raramente eclodem casos de discriminação algorítmica nos mais diversos setores, que, sob o rótulo de equações matemáticas despersonalizadas, oprimem e violam direitos a partir do uso das TICs (Mulholland, 2018).

Cite-se, a exemplo, o episódio de grande repercussão que ocorreu com a empresa Amazon, no caso de recrutamento e seleção de candidatos a vagas de emprego, por meio do uso de *machine learning* e tomada de decisões automatizadas (Dastin, 2018). A ferramenta experimental de contratação da empresa usou inteligência artificial (IA) para dar aos candidatos às vagas de emprego, pontuações que variam de uma a cinco estrelas. Contudo, a Amazon percebeu que seu novo sistema promovia uma conduta sexista. Isto porque uma das formas de treinamento da IA era a análise de currículos de um banco de dados de dez anos que em sua maioria era composto dados de homens, fato que fazia a IA reconhecê-los como as melhores opções. Com efeito, o sistema da Amazon ensinou a si mesmo que candidatos do sexo masculino eram preferíveis, penalizando currículos que incluíam a palavra "feminino", como em "capitã do clube de xadrez feminino"[79]. Veja que o sistema da Amazon, utilizando tecnologias de correlação de dados, aplicou o chamado "efeito mosaico," segundo o qual, a combinação de múltiplas informações aparentemente “triviais” resultou na identificação de características sensíveis dos candidatos, como o gênero (Bioni, 2021).

A mesma situação pode ocorrer com outros "registros digitais", como o histórico de navegação, termos de pesquisa ou até mesmo compras realizadas por um consumidor. Esses dados têm o potencial de revelar diversos atributos da personalidade de um indivíduo, incluindo informações sensíveis. Nesse sentido, Stefano Rodotà (2008, p. 84) argumenta: "(...) seja porque dados pessoais, aparentemente não sensíveis, podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando a pessoa pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas."

Portanto, a proteção de dados pessoais está intrinsecamente ligada à tutela do princípio da isonomia (Doneda, 2020), funcionando como um instrumento de contenção contra práticas discriminatórias. Em vista disso, a LGPD adota um regime jurídico mais protetivo em relação a dados sensíveis[80], visando a mitigar práticas discriminatórias.

---

[79] Na língua inglesa, não existe diferenciação de locução verbal entre feminino e masculino. Isso significa que os verbos não mudam de forma com base no gênero do sujeito, por essa razão o sistema da Amazon passou a identificar mecanismos que pudessem predizer o gênero do candidato (Dastin, 2018).

[80] Veja, nesse sentido, a seção II da LGPD.

Por essa razão, a proteção dos dados pessoais tem um papel de fundamental importância para que o cidadão "se realize e se relacione" na sociedade, característica essencial dos direitos da personalidade (Bandeira de Mello, 2009).

2.1.2.2 IoT e a "dataficação" de tudo

A característica da ubiquidade da *internet* já foi abordada anteriormente ao se discutir o crescimento exponencial dos *smartphones* no contexto nacional (*Vide Capítulo 1.2.3*). É nesse cenário que emerge o denominado fenômeno da dataficação**:** o ato de dataficar – pôr em dados – praticamente toda a vida de uma pessoa.

Para além dos *smartphones*, espera-se que os mais diversos objetos estejam conectados à *internet* (Bioni, 2021). É a chamada "*internet* das coisas" (IoT), conceituada por Eduardo Magrani (2018) como sendo objetos físicos interconectados com a rede mundial de computadores por meio de sensores embutidos, criando um ecossistema de computação onipresente com o intuito de facilitar o cotidiano das pessoas.

Tais características da tecnologia IoT tendem a integrar tudo aquilo antes considerado exclusivo do mundo *offline* ao mundo *online* e, como consequência, são produzidos mais dados.

Em todos os ambientes e aspectos da vida cotidiana, os chamados dispositivos inteligentes (*smart devices*) tomam as mais diversas formas, desde a automação domésticas - como assistentes virtuais (*e.g., Amazon Echo*) ou geladeiras inteligentes (*e.g., Samsung RF28HMELBSR/AA*) –, passando por roupas (*e.g., Al Pin*) e acessórios (*e.g., smartwatches),*etc. (Magrani, 2018). Concretiza-se, assim, o caráter da *ubiquidade computacional* prevista por Mark Weiser (1991) na década de 1990.

Como consequência desse contexto, há um aumento exponencial da coleta de dados pessoais, fazendo com que o ser humano tenha suas individualidades – como hábitos alimentares, padrões de sono, rotinas de exercícios, localização geográfica e até preferências de entretenimento e vestuário –, cada vez mais dataficadas.

Cria-se, portanto, uma verdadeira "biografia digital"[81] dos usuários. Nesse sentido, problematiza-se, mais ainda, o desafio da tutela dos dados pessoais como um novo direito da personalidade, visto que, muitos aspectos da vida de uma pessoa poderão ser decididos a partir de sua extensão eletrônica (Bioni, 2021).

[81] Daniel James Solove (2004) utilizou a expressão "biografia digital" ao tratar do fenômeno da dataficação.

2.1.2.3 A "câmara de eco digital"

As TICs não apenas capturam vastas quantidades de dados pessoais dos usuários. Também classificam e segmentam essas informações (*Vide Capítulo 1.2.2*). Esse processo culmina na criação de estereótipos, determinantes para calibrar uma série de decisões algorítmicas que influenciam "oportunidades sociais" no contexto da *data-driven economy* (Solove, 2004).

A consolidação das TICs trouxe consigo mudanças profundas na forma como nos relacionamos com o mundo e, em especial, com a informação. Anteriormente à *internet*, a comunicação era predominantemente unidirecional e limitada à transmissão de informações sobre eventos ou indivíduos, geralmente por meio de veículos como rádio, televisão e jornal impresso. Essas informações chegavam aos destinatários com um atraso temporal significativo, uma vez que o fluxo comunicativo era centralizado e dependente de intermediários que controlavam a produção e distribuição das notícias. Em contraste, o cenário informacional contemporâneo, impulsionado pela *internet*, possibilita uma comunicação multilateral e em tempo real, a partir de que múltiplos emissores podem se comunicar simultaneamente com diversos destinatários em escala global, rompendo barreiras temporais e geográficas (Castells, 2003).

Diante da escalada na capacidade de processamento de informações (*e.g., big data*) no contexto da "sociedade da informação", a tarefa de examinar essa imensidão informativa em busca das partes realmente importantes ou apenas relevantes exige, por parte do usuário, dedicação extensiva e integral. Por essa razão, Eli Pariser (2012) argumenta que, os seres humanos são cada vez mais incapazes de dar conta de tanta informação. Nesse contexto, os filtros de personalização se apresentam, a *priori*, como a solução ideal ao criar um "mundo sob medida, adaptado à perfeição para cada um de nós" (Pariser, 2012, p. 16).

Eli Pariser, em seu livro *"The filter bubble"* (2012), discute como essa personalização gera o fenômeno da "bolha informacional" – ou "bolha dos filtros" em tradução literal –, na qual os indivíduos são expostos a uma realidade informacional restrita e tendenciosa. Esse isolamento informacional apresenta uma série de riscos tanto para a liberdade de pensamento quanto para a coesão social. Nesse sentido, aduz John Stuart Mill, citado por Eli Pariser (2012, p. 55):

> Não há como enfatizar suficientemente a importância (…) de colocar os seres humanos em contato com pessoas diferentes de si mesmos, com modos de pensamento e ação distantes daqueles com os quais estão familiarizados. (…) Esse tipo de comunicação sempre foi e continua a ser, especialmente na era atual, uma das principais fontes de progresso.

A personalização digital visa a adaptar o conteúdo *online* às preferências de cada usuário, criando uma "rede sob medida"[82] (Castells, 2005, p. 23). Esse processo, movido por algoritmos que extrapolam os gostos e comportamentos individuais, molda um ambiente informativo de acordo com os cliques e interações anteriores do usuário. Embora essa adaptação tenha a vantagem de otimizar o tempo e facilitar a busca de informações, ela também provoca o isolamento do usuário em uma "câmara de eco digital"[83], em que apenas ideias semelhantes são reforçadas. Isso impede o acesso a informações contrárias ou divergentes, essencial para o desenvolvimento intelectual e a manutenção de uma sociedade democrática saudável (Pariser, 2012). Nesse sentido, complementa Eli Pariser (2012, p. 62):

> A bolha dos filtros tende a amplificar drasticamente o viés da confirmação, de certa forma, é para isso que ela serve. O consumo de informações que se ajustam às nossas ideias sobre o mundo é fácil e prazeroso; o consumo de informações que nos desafiam a pensar de novas maneiras ou a questionar nossos conceitos é frustrante e difícil. É por isso que os defensores de uma determinada linha política tendem a não consumir a mídia produzida por outras linhas. Assim, um ambiente de informação baseado em indicadores de cliques favorece o conteúdo que corrobora nossas noções existentes sobre o mundo, em detrimento de informações que as questionam.

O impacto da (hiper)personalização afeta a identidade individual e coletiva. Daniel James Solove (2004) destaca que a segmentação baseada em dados fragmentados cria uma versão estática e limitada de quem somos, reduzindo a plasticidade necessária para a evolução pessoal. Os algoritmos não apenas respondem ao comportamento do usuário, mas também moldam esse comportamento, criando um ciclo vicioso em que o passado define rigidamente o presente e o futuro. O usuário é, assim, encarcerado em uma versão informacional de si mesmo, sem espaço para crescimento ou mudança, o que Pariser (2012) convencionou chamar de "determinismo informativo".

---

[82] A expressão "rede sob medida" refere-se à capacidade dos indivíduos e organizações de personalizarem suas interações e fluxos de informação dentro da "sociedade em rede" de Castells. Enquanto Castells (2002) destaca a flexibilidade e globalidade das redes digitais, "rede sob medida" enfatiza a adaptação dessas redes às necessidades e interesses específicos, permitindo uma experiência comunicativa personalizada na era digital.

[83] A expressão "câmara de eco digital" refere-se ao ambiente *online* em que os usuários, ao interagir com conteúdos e pessoas que compartilham visões semelhantes, acabam por ouvir repetidamente as mesmas ideias, opiniões e informações. O termo "eco" é utilizado para destacar essa repetição, assim como o eco em um ambiente físico reflete o som, reforçando as mesmas mensagens sem introduzir novidades ou diferentes perspectivas. Dessa forma, o ambiente digital se torna fechado e autorreferencial, limitando o debate e a diversidade de opiniões.

Em suma, no contexto do *big data*, são os dados que passam a orquestrar (Pariser, 2012) as vidas dos usuários, decidindo a respeito de suas oportunidades (*Vide Capítulo 1.3.2*), o que Viktor Mayer-Schönberger e Keller Cukier (2014) convencionaram chamar de "ditadura dos dados"[84].

2.1.3 Proteção de dados como categoria autônoma dos direitos da personalidade

A proteção de dados pessoais consolida-se como uma categoria autônoma dos direitos da personalidade, transcendendo a esfera da privacidade para incluir o controle sobre a circulação e o uso das informações pessoais. Nesse sentido, a proteção de dados assume uma dimensão normativa própria, orientada pela autodeterminação informativa, essencial à preservação da dignidade e da identidade do indivíduo na "sociedade da informação", em que os limites entre o público e o privado estão em constante redefinição.

2.1.3.1 Rompendo com a dicotomia do público e do privado

Segundo Stefano Rodotà (2008), o surgimento da privacidade não se apresenta como uma exigência "natural" de cada indivíduo, mas como a aquisição de um privilégio por parte de determinados grupos. Para compreender essa perspectiva, é necessário considerar o contexto socioeconômico em que amadureceram as condições que fundamentaram a afirmação da privacidade como uma demanda que exige tutela autônoma (Rodotà, 2008).

Hannah Arendt (2007) argumenta que o surgimento da sociedade moderna transformou a distinção entre as esferas pública e privada, especialmente com o avanço das dinâmicas sociais associadas à "sociedade de massas". Nesse novo contexto, o espaço privado foi progressivamente invadido por tendências conformistas[85], dificultando a separação entre essas esferas (Arendt, 2007). Arendt (2007) observa que a igualdade moderna, sustentada pelo conformismo e pela prevalência do comportamento sobre a ação como forma de interação

[84] Mayer-Schönberger e Cukier (2014) alertam para o risco de uma "ditadura de dados," em que a fetichização da informação e dos resultados das análises pode levar ao uso inadequado dos dados. Os autores destacam que os perigos de não regular o *big data*, especialmente em relação à privacidade e previsões, são maiores do que se imagina e vão além de temas triviais, como anúncios direcionados *online*.

[85] O conformismo, na filosofia de Hannah Arendt, pode ser definido como a tendência moderna de buscar uma igualdade baseada no ajustamento dos comportamentos individuais a padrões estabelecidos, resultando em uma conformidade coletiva que elimina a singularidade e espontaneidade dos indivíduos.

humana, difere radicalmente da concepção antiga, em que a esfera pública era o espaço da individualidade e do autêntico reconhecimento de cada indivíduo.

A "sociedade de massas", com suas características de controle social, suprimiu a autonomia do indivíduo[86] e redesenhou os contornos da esfera privada (Arendt, 2007). Em vista disso, a privacidade emerge nesse (novo) contexto como essencial ao livre desenvolvimento da personalidade do cidadão, uma vez que, somente com a "fuga da pressão social", os indivíduos podem desenvolver cada qual sua subjetividade(Arendt, 2007) para, posteriormente, projetá-la em meio à sociedade (Bioni, 2021).

Arendt (2007) observa que a distinção entre as esferas pública e privada, sob a ótica da privacidade e não do corpo político, consiste na diferenciação entre o que deve ser exposto e o que deve permanecer oculto. Nessa perspectiva, a proteção da intimidade ganha legitimidade, pois a individualidade de cada pessoa deve ser compartilhada conforme sua escolha pessoal[87], permitindo que ela construa e projete sua personalidade socialmente, em seu próprio ritmo. Nesse contexto, a privacidade emerge como o direito de "estar só"[88], protegido de interferências externas, e de manter em segredo certos aspectos de sua vida. Essa dicotomia entre as esferas pública e privada é essencial para garantir a liberdade individual e salvaguardar o indivíduo contra intrusões indesejadas (Lafer, 2005).

O artigo seminal "*the right to privacy*", escrito pelos advogados Warren e Brandeis em 1890, marcou um ponto crucial no debate sobre a inviolabilidade da vida privada, ao propor limites claros à intromissão pública nesse âmbito. A motivação para a obra teria origem na própria experiência de Warren, que enfrentou um escândalo envolvendo sua vida conjugal. Ele havia se casado com a filha de um senador de uma tradicional família de Boston, enquanto sua

---

[86] Arendt (2007) observa que, no "*behaviorismo"*, conforme aumenta o número de pessoas, também cresce a probabilidade de que elas se comportem de maneira uniforme, reduzindo a tolerância ao não-comportamento. Com isso, os feitos perdem gradualmente sua capacidade de oposição e os eventos, seu potencial de iluminar e dar sentido ao tempo histórico.

[87] Conforme Celso Lafer (2005), a proteção da intimidade, a partir do que expressa Arendt com base nas ideias de Kant, busca assegurar a identidade do indivíduo em meio aos riscos decorrentes da pressão uniformizadora da sociedade e da imposição do poder político. Esse princípio de exclusividade é caracterizado pelo que passa pelas escolhas pessoais e pela subjetividade, elementos que não são regulados por normas ou padrões objetivos. Assim, a exclusividade compreende três aspectos centrais: a solidão, que reflete o desejo de estar só; o segredo, que justifica a necessidade de sigilo; e a autonomia, que representa a liberdade do indivíduo de decidir sobre si mesmo como fonte originária de suas próprias informações.

[88] A expressão "direito de estar só", conforme interpretada por Bulos (2008), refere-se à proteção da vida privada e da intimidade, que são vistas como aspectos essenciais desse direito. Para Bulos, esse conceito assegura a esfera pessoal do indivíduo, protegendo-o contra interferências externas. Essa ideia encontra paralelo no termo "*riservatezza*" na Itália e "*privacy*" nos Estados Unidos, ambos destinados a garantir que certos aspectos da vida humana permaneçam invioláveis e livres de invasões.

vida luxuosa e desordenada chamou atenção, tornando-o alvo de críticas e exposições públicas (Nojiri, 2005).

O comando de que a vida privada é inviolável[89] resulta da rivalização entre as esferas do público e do privado. Nessa trama, o que é público e privado é o que normatiza o conteúdo do direito à privacidade, sendo a sua lógica centrada na "liberdade negativa"[90] de o indivíduo não sofrer interferência alheia (Bioni, 2021).

No contexto da "sociedade da informação", em que o fluxo informativo é intensamente redimensionado e virtualizado, a linha divisória entre público e privado se torna fluida e constantemente diluída (Rodotà, 2008). A privacidade, que antes representava apenas o controle sobre a divulgação de informações pessoais, agora se estende ao domínio da circulação dessas informações no meio digital. Stefano Rodotà (2008) observa que, nesse cenário, não é mais possível compreender a privacidade dentro da lógica simplista do "apresentar-se" e "esconder-se", pois essa abordagem binária entre recolhimento e exposição, ou entre a "casa-fortaleza", que enaltece a privacidade, e a "casa-vitrine", que valoriza as trocas sociais, tornou-se insuficiente. Stefano Rodotà (2008) enfatiza que essas dicotomias tradicionais se revelam cada vez mais abstratas, refletindo uma visão que deixa de lado a urgência de expandir o conceito de privacidade para além de um âmbito meramente individualista, restrição que caracterizava suas origens.

Esse processo evolutivo do direito à privacidade compreenderia, portanto, a proteção de dados pessoais, sob uma perspectiva de proteção "dinâmica" e em uma "liberdade positiva"[91] do controle sobre informações pessoais, o que, no entanto, não significa que o direito à proteção de dados deveria ser reduzido à uma mera evolução do direito à privacidade (Rodotà, 2008).

Nesse contexto, o conceito de proteção de dados pessoais se configura como um direito autônomo (Bioni, 2021), distinto do direito à privacidade, e expande-se para além da dicotomia

---

[89] Nesse sentido aduz o art. 5°, X, da CF (1988): "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; Art., 21 do CC: "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma".

[90] De acordo com Isaiah Berlin (2002), a liberdade negativa é entendida como a ausência de interferência ou impedimentos externos que limitem as possibilidades de escolha dos indivíduos. Esse conceito de liberdade refere-se à tentativa de garantir que o indivíduo esteja livre de qualquer restrição externa, assegurando um espaço em que possa agir de acordo com sua própria vontade, sem interferências arbitrárias. Nesse sentido, a liberdade negativa representa uma proteção contra invasões à autonomia pessoal.

[91] Isaiah Berlin (2002) descreve a liberdade positiva como o poder de agir ou pensar de acordo com sua própria autodeterminação, sendo "senhor de si mesmo", responsável por suas escolhas. Diferente da liberdade negativa, que busca a ausência de interferência, a liberdade positiva está associada à capacidade de o indivíduo realizar suas ações de forma autônoma, participando ativamente de sua vida e do ambiente ao seu redor. Essa noção envolve a libertação para agir de forma autêntica, com a possibilidade de justificar suas decisões com base em seus próprios valores e objetivos.

público-privado, abrangendo o controle sobre as informações pessoais em todas as instâncias de circulação (Rodotà, 2008). Essa evolução, conforme analisado por Rodotà, reflete uma nova dimensão da relação da pessoa com a sociedade, a partir de que a autodeterminação informativa assume papel central (Rodotà, 2008). O controle sobre os dados pessoais ultrapassa a simples defesa contra invasões à privacidade, constituindo-se como uma extensão da liberdade individual em um ambiente altamente digitalizado (Bioni, 2021). Esse contexto digital impõe uma dinâmica própria e desafios inéditos à proteção humana, já que os dados não apenas prolongam a identidade individual, mas também interferem diretamente em sua esfera relacional (*Vide Capítulo 2.1.1.2*). Dessa forma, a normatização específica se torna imprescindível, justificando dogmaticamente a autonomia do direito à proteção de dados pessoais e suas implicações jurídicas (Doneda, 2019)[92].

A proteção de dados, ao assumir a condição de direito independente, demanda uma especificidade normativa, que permita não só garantir a privacidade[93], mas também regular o uso, o tratamento, a circulação e o armazenamento de informações em um mundo digital em que o fluxo de dados transcende as divisões clássicas de espaço público e privado, além de, (re)configurar uma nova dinâmica mercadológica (*Vide Capítulo 1.2*) (Bioni, 2021).

2.1.3.2 Autodeterminação informacional: a dupla função das leis de proteção de dados pessoais.

O poder econômico e o avanço tecnológico têm historicamente se posicionado como forças contrárias na defesa dos direitos humanos. Nesse sentido, Norberto Bobbio (2004, p. 209) observa que:

> (...) a luta pelos direitos teve como primeiro adversário o poder religioso; depois, o poder político; e, por fim, o poder econômico. Hoje, as ameaças à vida, à liberdade e à segurança podem vir do poder sempre maior que as conquistas da ciência e das aplicações que dela derivadas dão a quem está em condição de usá-las. Entramos na era que é chamada de pós-moderna e é caracterizada pelo enorme progresso, vertiginoso e irreversível, da transformação tecnológica e, consequentemente,

[92] Frazão e Carvalho (2018) discutem o direito fundamental à proteção de dados pessoais em um cenário no qual o uso massivo de dados pelos gigantes da *internet* impõe novos desafios à integridade e autonomia do indivíduo. Eles destacam que essa proteção possui duas dimensões: uma subjetiva, que confere ao indivíduo um direito de defesa contra os riscos à sua personalidade oriundos da coleta e manipulação de dados; e uma objetiva, que exige uma atuação protetiva do Estado para garantir o controle sobre os fluxos de informações pessoais.

[93] Bioni (2021) argumenta que o direito à proteção de dados pessoais envolve um conjunto de liberdades individuais que não se esgotam no âmbito do direito à privacidade. Ele observa que o núcleo central da proteção de dados pessoais se distingue da privacidade, uma vez que sua tutela jurídica transcende a tradicional dicotomia entre esferas pública e privada.

> também tecnocrática do mundo. Desde o dia em que Bacon disse que ciência é poder, o homem percorreu um longo caminho! O crescimento do saber só fez aumentar a possibilidade de o homem dominar a natureza e os outros homens.

Esse pensamento expressa uma preocupação crucial na contemporaneidade: a forma como o poder econômico, impulsionado pelos avanços tecnológicos na "sociedade da informação", pode comprometer o livre desenvolvimento da personalidade dos indivíduos, intensificando sua vulnerabilidade diante de uma sociedade cada vez mais refém e dependente desse livre fluxo informativo[94] (*Vide Capítulo 1.3.2*) (Bioni, 2021).

No contexto da *data-driven economy*, os dados pessoais emergem como um recurso estratégico valioso, concentrando poder nas mãos das corporações tecnológicas (Frazão; Oliva; Tepedino, 2019). Shoshana Zuboff (2021) esclarece que o "capitalismo de vigilância" age por meio de assimetrias[95] nunca antes vistas referentes ao conhecimento[96] (*Vide Capítulo 1.2.2*) e ao poder que dele resulta, embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como "superávit comportamental" do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" – o novo meio de produção – e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde.

No contexto atual, caracterizado pelo processamento massivo de dados viabilizado pelo *big data*, IA e algoritmos preditivos, as corporações conseguem não apenas otimizar processos produtivos, mas também aprimorar a tomada de decisões estratégicas[97] (*Vide Capítulo 1.2.1*).

---

[94] Segundo Doneda (2019), é possível observar que a herança cultural e histórica que nos antecede evidencia a complexidade de se compreender o progresso de maneira unilateral ou unificada nos dias atuais. Inicialmente, a ideia de progresso possuía um caráter universalista, mas com o tempo esse universalismo foi se dissipando. Baumann (2001) acrescenta que o progresso, assim como outros aspectos da vida moderna, passou por um processo de desregulamentação, por meio do qual a avaliação de uma "novidade" é realizada de forma livre e individual, e também de privatização, no sentido de que se espera que cada pessoa, individualmente, utilize seus próprios recursos para alcançar uma condição mais satisfatória, superando, assim, eventuais condições desfavoráveis.

[95] Nesse sentido, as *big techs* apropriam-se da experiência humana quando o usuário "cede gratuitamente suas informações ao concordar com termos de uso, utilizar serviços gratuitos ou simplesmente circular em espaços onde as máquinas estão presentes" (Koerner, 2021, p. 01).

[96] Nesse sentido, os dados podem ser entendidos como fatos brutos, coletados e armazenados em formato eletrônico ou digital, com valor agregado limitado e dependente de tratamento para extração de significado e utilidade. Assim, o dado constitui a matéria-prima da informação, que, por sua vez, resulta do tratamento aplicado a uma base de dados específica (*Vide Capítulo 1.2.2*).

[97] As tecnologias persuasivas, utilizadas pelos capitalistas de vigilância para capturar a atenção dos usuários e influenciar comportamentos, têm sido desenvolvidas para afetar processos psicológicos e de cognição social de forma sutil e inconsciente, conduzindo a mente do usuário a operar de modo automatizado (Felipe, 2023). Esse conceito, denominado *mindless computing*, visa a facilitar a experiência do usuário, tornando as tarefas desejadas mais acessíveis e fáceis de realizar (Joaquim, 2021). A intenção é manter o usuário conectado, pois quanto maior o engajamento, maior a captação de dados (Senra, 2020) e maior a exposição às técnicas de *marketing* que estimulam a aquisição de produtos e serviços (Brito; Silva, 2020).

Esse modelo, no entanto, limita significativamente o controle individual sobre dados pessoais, gerando preocupações éticas substanciais em torno de privacidade e autonomia, à medida que as empresas extraem valor econômico da exploração contínua dessas informações (Zuboff, 2021). Nesse cenário de assimetria informacional, o princípio de "autodeterminação informacional" se apresenta como uma resposta jurídica e normativa essencial, buscando reequilibrar essa relação ao assegurar aos indivíduos o poder sobre o uso e o destino de suas próprias informações (De Souza; Silva, 2020).

Historicamente, a proteção dos dados pessoais tem sido compreendida como o direito do indivíduo de autodeterminar as suas informações pessoais – autodeterminação informacional (Bioni, 2016). No entanto, o simples reconhecimento deste direito não é suficiente para garantir uma proteção efetiva, uma vez que o poder das corporações e o desequilíbrio na relação entre titulares e controladores de dados minam a capacidade de controle real dos indivíduos sobre suas informações (De Souza Santos, 2023). Este cenário reflete a tensão entre a autonomia individual e o poder econômico, exacerbada pelas novas tecnologias que permitem uma coleta massiva e tratamento automatizado de dados (Doneda; Sarlet; Mendes, 2022).

É nesse contexto que a dupla função das leis de proteção de dados pessoais ganha relevância. Além de proteger os direitos fundamentais à privacidade e à autodeterminação informacional, tais legislações também desempenham um papel crucial no fomento ao desenvolvimento econômico (Bioni, 2021). A proteção de dados não deve ser vista apenas como uma barreira ao progresso tecnológico ou econômico, mas como um mecanismo que equilibre o poder entre indivíduos e corporações, criando condições mais justas para o desenvolvimento da economia digital (Bioni, 2022).

Essas leis cumprem, assim, duas funções essenciais: à proteção de direitos e o incentivo ao desenvolvimento econômico[98]. A proteção de direitos busca evitar a exploração indevida dos dados pessoais, preservando a privacidade e a autonomia dos indivíduos, com o consentimento como principal instrumento de controle (Bioni, 2021).

[98] Não é sem razão que a LGPD, logo em seus artigos iniciais, tem o cuidado de prever expressamente os seus propósitos e valores principais, nos seguintes termos: Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; **II – a autodeterminação informativa**; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – à inviolabilidade da intimidade, da honra e da imagem; **V – o desenvolvimento econômico e tecnológico e a inovação;** VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Do ponto de vista econômico, um ambiente regulatório adequado em proteção de dados fortalece a confiança dos consumidores e estimula a inovação, incentivando práticas éticas e sustentáveis, fundamentais ao crescimento de setores como *marketing* digital e inteligência artificial (Cruz, 2024). Dessa forma, a legislação de proteção de dados opera como o fiel da balança entre a defesa dos direitos individuais e o progresso econômico, promovendo um uso ético dos dados que favoreça tanto a autodeterminação informacional quanto o desenvolvimento econômico inclusivo e sustentável.

2.2 A TRAVESSIA DO PROTAGONISMO DO CONSENTIMENTO

A criação de um sólido conjunto de normas para a proteção de dados pessoais foi um processo gradual, resultado de anos de discussões, debates e documentos que pavimentaram o caminho para o que se tem atualmente (Lugati; De Almeida, 2020). A partir de uma variedade de interpretações sobre o conceito de privacidade[99], e apesar das diferenças entre os sistemas jurídicos, houve uma convergência que levou à formulação de leis específicas para a proteção de dados[100]. Esse movimento é uma resposta ao processo de transformação digital que está moldando o ambiente regulatório e afetando significativamente o mercado (Mendes; Da Fonseca, 2020).

A acelerada transformação tecnológica tem frequentemente revelado a inadequação do arcabouço legal tradicional em face do aumento exponencial do uso de dados pessoais (Rodotà, 2008). Essa dinâmica impôs a necessidade de uma abordagem jurídica mais refinada e especializada, demandando das ciências jurídicas e de seus profissionais a criação de normas e regulamentos que atendam às demandas contemporâneas da sociedade. Assim, buscou-se garantir um equilíbrio adequado entre a proteção dos direitos dos indivíduos e o uso legítimo

[99] A concepção de privacidade evoluiu historicamente de um direito negativo, centrado na não interferência estatal, para uma necessidade de proteção específica diante do avanço das tecnologias invasivas. Iniciada com o marco de Warren e Brandeis em "*The right of privacy"* e o conceito de "*right to be let alone*" de McIntyre, a privacidade passou de uma defesa individualista para um conceito ampliado. Com o surgimento do processamento informatizado de dados, especialmente a partir de 1960, tornou-se necessário redefinir esse direito para abranger a proteção de dados pessoais (Doneda, 2020). Nos anos 1970, decisões jurídicas começaram a tratar os dados pessoais como projeções da personalidade do indivíduo, legitimando sua tutela jurídica (Mendes, 2014). Essa trajetória resultou em legislações específicas, como a LGPD e a GDPR, que consolidam a proteção de dados como um direito fundamental, refletindo a ampliação progressiva das normas para acompanhar o impacto das tecnologias modernas (Lugati; De Almeida, 2020).

[100] As doutrinas defendem a visão de Viktor Mayer-Schönberger, que propõe que a regulamentação da proteção de dados pessoais percorreu quatro gerações distintas, que, de acordo com Doneda (2011, p. 96), são "leis que partem de um cerne mais técnico e restrito para, por fim, ampliar as disposições e as técnicas referentes às tecnologias modernas".

de dados pessoais (Mendes; Da Fonseca, 2020). Contudo, o estabelecimento de um regime regulatório robusto e eficaz não foi imediato, exigindo anos de aprofundamento, pesquisas e debates sobre o tema.

2.2.1 Quatro gerações de leis de proteção de dados pessoais[101] e o consentimento

A proteção de dados pessoais surge como uma resposta às tentativas dos governos, nas décadas de 1960 e 1970, de centralizar informações sobre cidadãos em grandes bancos de dados nacionais, como o "*National Data Center*" nos Estados Unidos e o projeto SAFARI na França (Doneda, 2020). Impulsionadas pelo avanço da ciência computacional, essas iniciativas visavam a melhorar a eficiência administrativa por meio do acesso integrado a dados (Bioni, 2021). No entanto, a reação popular levantou preocupações sobre privacidade e controle estatal, dados os riscos de concentração de poder sobre informações individuais (Mendes, 2008). Essa resistência motivou o desenvolvimento inicial de normas de proteção de dados, favorecendo o processamento descentralizado e a adoção de identificadores setoriais em vez de números universais, demonstrando uma convergência internacional na regulamentação de dados com foco na privacidade diante das inovações tecnológicas (Mendes, 2008).

A "primeira geração" de leis de proteção de dados[102] foi estruturada para mitigar os riscos associados ao processamento eletrônico massivo de dados pessoais pela Administração Pública, refletindo a preocupação popular de um poder absoluto de uma burocracia automatizada e desumanizada (Mendes, 2008). A falta de experiência no tratamento com (novas) tecnologias ainda pouco familiares, aliada ao receio de um uso indiscriminado destas, sem que se soubesse ao certo suas consequências, fez com que se optasse por um controle

[101] Optou-se por seguir a taxonomia desenhada por Viktor Mayer-Schönberger (1997), que estabelece quatro divisões, histórico-evolutivas, para as gerações de leis de proteção de dados pessoais. Adota-se na presente pesquisa, uma abordagem mais descritiva, objetivando traçar como o consentimento está inserido nesse processo.
[102] São exemplos de normas da primeira geração as seguintes: as leis do Estado alemão de *Hesse* (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de dados alemão de *Rheinland-Pfalz* (1974) e a Lei Federal de Proteção de Dados da Alemanha.

baseado em um regime de autorizações[103], rígido[104] e detalhado, que demandava um minucioso acompanhamento (Doneda, 2020).

As normas da primeira geração logo se mostraram insuficientes diante da expansão tecnológica e da descentralização do processamento de dados (Mendes, 2008). O modelo centralizado foi superado pela possibilidade de pequenos órgãos públicos e privados gerenciarem informações de forma autônoma, o que evidenciou a fragilidade de uma regulamentação pautada em autorizações rígidas e procedimentos formais, sem foco direto na proteção de direitos (Bioni, 2021).

O temor de um banco de dados único e centralizado foi substituído pelo receio da proliferação de inúmeros bancos de dados interconectados globalmente (Mendes, 2008). Essa mudança evidenciava a insatisfação dos cidadãos com o uso indiscriminado de suas informações pessoais, sem mecanismos eficazes de defesa. Diante da fragmentação dos polos de tratamento, o modelo rígido das leis anteriores tornou-se inviável, impulsionando um sistema que permite ao indivíduo identificar e questionar o uso de seus dados – "segunda geração" de leis de proteção de dados[105] (Doneda, 2020). As técnicas de controle, então, adaptaram-se ao novo contexto, com o mecanismo de autorização de funcionamento de bancos de dados sendo substituído por simples notificações de criação, enquanto as autoridades de controle assumiram funções de mediação e apoio à administração pública, atuando como órgãos para-jurisdicionais ou *ombudsman*[106] (Mayer-Schönberger, 1997).

Estas leis apresentavam igualmente seus problemas, o que levou a uma mudança de paradigma, pois se reconheceu que fornecer esses dados havia se tornado essencial para a participação social. Tanto o Estado quanto os entes privados passaram a depender do fluxo dessas informações para funcionar, e qualquer interrupção desse processo pelo cidadão poderia resultar em sua exclusão social (Mendes, 2008). Mayer-Schönberger observou que essa liberdade de interromper o fluxo de dados pessoais, em seu limite extremo, seria exequível

---

[103] Em conformidade com o que aduzem Danilo Doneda (2020) e Laura Schertel Mendes (2008), adotam-se, neste primeiro momento, regimes de autorização e modalidades de tratamento de dados a serem determinados *ex ante*, condicionando seu funcionamento à licença prévia ou ao registro nos órgãos competentes, sem prever a participação do cidadão nesse processo. Veja, nesse sentido: Viktor Mayer-Schönberger. "*General Development of Data Protection in Europe*. In: AGRE, Philip; ROTENBERG, Marc. (org.). *Technology and Privacy: The New Landscape. Cambridge: MIT Press*, 1997. p. 223-224".

[104] Priorizou-se o controle rígido dos procedimentos, deixando para segundo plano a garantia do direito individual à privacidade (Mendes, 2008).

[105] São exemplos de normas da segunda geração a lei francesa "*Informatique et Libertés*" (1978) e a lei austríaca *"Datenschutzgesetz*" (DSG) (1978).

[106] O *ombudsman* é um profissional que atua como mediador entre uma organização e o público, recebendo e resolvendo reclamações, sugestões e críticas. O termo tem origem no sueco e significa "representante do cidadão".

apenas para indivíduos que optassem por um isolamento social (Mayer-Schönberger, 1997). Assim, percebeu-se que essa liberdade individual impactava não apenas as informações pessoais, mas também a socialização de cada indivíduo (Doneda, 2020).

A “terceira geração” de leis de proteção de dados avançou para uma tutela mais sofisticada, indo além da mera liberdade de fornecimento de informações. Essas leis tratam a proteção de dados como um processo complexo, que inclui a participação ativa do indivíduo na sociedade e leva em conta o contexto em que os dados são solicitados, assegurando proteção quando a liberdade de escolha é limitada (Doneda, 2020). Inspiradas pela decisão do Tribunal Constitucional Alemão de 1983, que reconheceu o direito à autodeterminação informativa ao declarar inconstitucional a "Lei do Censo"[107], essas normas promovem o envolvimento contínuo do cidadão em todas as etapas do tratamento de seus dados, da coleta à transmissão (Mendes, 2008).

A transformação tecnológica das redes e telecomunicações também influenciou essas normas, ao tornar o armazenamento e a transmissão dos dados mais difusos e de localização menos identificável. Esse contexto de proliferação de bancos de dados interligados exigiu adaptações legais em países como Alemanha, Áustria e Noruega, que passaram a enfrentar a realidade descentralizada dos dados (Mendes, 2008).

Contudo, o ideal de participação ativa e contínua no controle dos dados mostrou-se desafiador na prática. Muitos cidadãos optaram por não exercer sua autodeterminação informativa devido aos altos custos econômicos e sociais, como a exclusão de serviços, restringindo o exercício desse direito a uma minoria disposta a enfrentar esses obstáculos (Doneda, 2020). Assim, apesar de buscar maior proteção e engajamento cidadão, a “terceira geração” de leis destacou as dificuldades de equilibrar o direito à privacidade com a complexidade tecnológica e social do período (Mendes, 2008).

A “quarta geração” de leis de proteção de dados surge como uma resposta pragmática às limitações das abordagens individuais das gerações anteriores, focando na criação de instrumentos que elevem o padrão geral de proteção (Bioni, 2021). Essas normas reconhecem que, para garantir a segurança dos dados pessoais, não basta contar apenas com a escolha

[107] Para Viktor Mayer-Schönberger (1997), a decisão do Tribunal Constitucional Alemão sobre a Lei do Censo Alemã (*Volkszählungsgesetzes*) marcou um ponto de inflexão na proteção de dados pessoais. A lei, que obrigava os cidadãos a fornecerem uma ampla gama de informações ao governo, suscitou preocupações sobre privacidade e controle estatal. O Tribunal considerou que a obrigatoriedade desse fornecimento de dados, sem garantias adequadas de proteção, violava o direito constitucional à autodeterminação informativa dos cidadãos. Em consequência, essa decisão fundamentou emendas significativas às leis de proteção de dados na Alemanha e Áustria e inspirou legislações específicas em países como Noruega e Finlândia, consolidando o princípio de que determinados dados exigem um nível de proteção que não pode depender apenas da escolha individual.

individual; é necessário proteger contra o desequilíbrio na relação entre o indivíduo e as entidades que coletam e processam suas informações (Doneda, 2020). Nesse sentido aduz Bruno Ricardo Bioni (2021, p. 116): "a disseminação de autoridades independentes para a aplicação as leis de proteção de dados pessoais, bem como de proposições normativas, que não deixavam ao reino do indivíduo a escolha sobre o processamento de certos tipos de dados pessoais (*e.g.,* dados sensíveis), relativizaram a referenciada centralidade do consentimento".

Outra característica dessa "quarta geração" é a adoção de regulamentações setoriais complementares, que ampliam a proteção em áreas específicas, como saúde e crédito ao consumo, ajustando os princípios gerais de proteção de dados às particularidades de cada setor[108] (Doneda, 2020).

Ainda assim, esse avanço geracional não afastou o consentimento do papel central na regulação de dados. Sua importância continuou a ser uma característica marcante da abordagem normativa, de modo que, ao longo desse processo evolutivo, o consentimento passou a ser qualificado como livre, informado, inequívoco, explícito e específico, especialmente no direito comunitário europeu[109]. Essa definição detalhada reforça o protagonismo do consentimento, equiparando-o ao conceito de autodeterminação informativa (Bioni, 2021).

2.2.2 A redoma do consentimento

Considerando a relevância fundamental do instituto do consentimento nas normas que versam sobre a proteção de dados pessoais, este item se propõe a examinar esse instituto nos principais diplomas europeus (reconhecidos como a base da proteção à autodeterminação informativa). Em seguida, analisam-se as normas brasileiras que antecederam a LGPD, abordando a legislação setorial, para, por fim, adentrar na análise da LGPD, recente marco no ordenamento jurídico nacional.

---

[108] Nesse sentido, conforme observa Danilo Doneda (2020), esse fenômeno não constitui exatamente uma "setorização" da disciplina de dados pessoais, embora tal risco deva ser considerado; trata-se, antes, de um instrumento que visa a assegurar a ampla eficácia dos princípios das leis de proteção de dados em contextos com especificidades próprias.

[109] No direito comunitário europeu, o consentimento ocupa uma posição central e é amplamente qualificado para assegurar a proteção efetiva dos dados pessoais. A Diretiva 95/46/CE, marco inicial da proteção de dados na União Europeia, já estabelecia que o consentimento deveria ser "livre, específico e informado" (Mendes, 2008), requisitos que foram reforçados e ampliados com o Regulamento Geral de Proteção de Dados (GDPR) em 2018, que exige também que seja "inequívoco" e, em certos casos, "explícito". Essas qualificações visam a garantir que os indivíduos tenham controle real sobre suas informações, fortalecendo a autodeterminação informativa, de modo que o consentimento não seja um mero ato formal, mas uma manifestação consciente e intencional.

2.2.2.1 Regulamentos fundamentais da União Europeia como pilares da proteção de dados

Apesar da existência de regulamentos anteriores que abordavam a proteção de dados pessoais e o instituto do consentimento[110], os países europeus — especialmente os membros da União Europeia — passaram a tratar do tema de forma intensiva a partir de 1980.

A Convenção 108, da década de 1980, *Strasbourg*[111], do Conselho da Europa, é resultado do movimento promovido pela OCDE[112] para facilitar a harmonização das legislações de proteção de dados pessoais (Bioni, 2021). Como observa Bruno Ricardo Bioni (2021), já no preâmbulo do tratado é destacada a relação entre a proteção de dados pessoais e o livro fluxo informacional transfronteiriço. Esta convenção teve uma influência significativa na elaboração da Diretiva Europeia de Proteção de Dados (95/46/EC), que de acordo com Doneda (2020), estabeleceu um modelo europeu caracterizado por uma abordagem abrangente e detalhada[113]. Esse modelo é integrado nas legislações nacionais de cada estado-membro, promovendo uma uniformização normativa em toda a União Europeia.

Para tornar o consentimento mais aplicável e efetivo, a diretiva europeia define que ele deve ser livre, informado, inequívoco e específico[114]. Essa qualificação marca um avanço significativo nas gerações das leis de proteção de dados, pois visa a enfrentar o problema de um controle limitado sobre as informações pessoais pelos próprios titulares (Bioni, 2021).

Além de reforçar o direito dos indivíduos ao controle de seus dados, a diretiva inova ao impor obrigações claras aos responsáveis pelo tratamento dos dados (*data controllers*)[115]. Ela

---

[110] Embora o "direito à privacidade" (*right to privacy*) tenha encontrado suas primeiras formulações teóricas e jurisprudenciais nos Estados Unidos, foi a Europa que se destacou ao consolidar um conjunto normativo robusto e abrangente para a proteção de dados pessoais, iniciado já nas décadas de 1970 e 1980. Em 1970, o estado alemão de Hesse promulgou a primeira lei específica sobre o tema. Em 1973, a Suécia aprovou o *Datalegen* (Lei 289 de 11 de maio), e, em 1977, a Alemanha sancionou sua lei federal para coibir o uso indevido de dados pessoais. A Dinamarca, em 1978, regulamentou a proteção de dados pessoais e corporativos com as Leis 243 e 244, enquanto a França, em 1978, promulgou a Lei 78-17 sobre a mesma matéria. Ainda, a Constituição Espanhola, em seu artigo 18, parágrafo 1º, impôs a necessidade de regulamentar a privacidade em face das tecnologias informáticas, e a Constituição Portuguesa de 1977 trouxe previsões específicas, como o direito de acesso, correção e atualização de dados pessoais (Reinaldo Filho, 2013).

[111] Disponível em: <http://conventions.coe.int/Treaty/en/Treatis/Html/108.htm>.

[112] A OCDE é um organismo internacional multilateral criado após a Segunda Guerra Mundial, em 1948, cuja missão é promover o bem-estar econômico e social global. Atualmente conta com 38 países-membros. O Brasil é um parceiro-chave da OCDE desde 2007, ao lado da China, Índia, Indonésia e África do Sul, e em 2022 tornou-se candidato à adesão à OCDE. Disponível em: <http://www.oecd.org/about/membersandpartners/>.

[113] Bioni (2021) ressalta que a Diretiva Europeia de Proteção de Dados (95/46/EC) deu forma concreta à promessa delineada pela Convenção de *Strasbourg*, ao estabelecer normas específicas para garantir aos indivíduos o controle sobre suas informações pessoais. Nesse contexto, a autodeterminação informacional do indivíduo surge como o critério central para determinar a licitude ou ilicitude de qualquer operação de tratamento de dados pessoais.

[114] Veja nesse sentido, os arts. 2(a), 7(a), 8(a).

[115] Isso pode ser observado na Seção VIII do mencionado diploma, que aborda a confidencialidade e a segurança no tratamento de dados.

também estabelece princípios[116] fundamentais que orientam a coleta, o tratamento e o uso dos dados, bem como práticas tecnológicas adequadas, promovendo uma abordagem mais rigorosa e ética de proteção (Krieger, 2019).

Enquanto as diretrizes da OCDE, atribuíam a responsabilidade de limitar o uso de dados exclusivamente ao titular, a Diretiva Europeia de Proteção de Dados (95/46/EC) avança ao estender esse dever de cooperação a todos os atores envolvidos no tratamento de dados. Essa distinção posiciona a diretiva na quarta geração das leis de proteção de dados, cuja característica marcante é o fortalecimento da autonomia do titular ao garantir-lhe maior controle sobre suas informações pessoais. Diferente das regulamentações anteriores, essa nova etapa normativa amplia seu alcance a todos os agentes que operam ao longo da cadeia de fluxo informacional, refletindo o caráter cada vez mais interconectado e complexo do cenário digital (Bioni, 2021) (*Vide Capítulo 2.2.1*).

Nesse contexto, a Diretiva Europeia (2002/58), voltada à proteção da privacidade nas comunicações eletrônicas, foi instituída para fortalecer ainda mais essa autonomia do titular no ambiente digital (Polčák; Kasl; Míšek, 2020). Suas disposições destacam a importância de um consentimento que seja livre, específico e informado, proporcionando ao indivíduo um controle mais efetivo sobre seus dados pessoais, preferencialmente antes da coleta e do processamento[117]. Para viabilizar esse controle, a diretiva recomenda o uso de medidas práticas, como "caixas de diálogo" nos *websites*, que permitam ao usuário manifestar seu consentimento de forma acessível e transparente. Entre as ferramentas de coleta mencionadas estão *cookies*, *web bugs* e *spywares*, promovendo uma maior transparência e controle sobre os dados no ambiente digital (Bioni, 2021).

A reforma subsequente das normas de proteção de dados, consolidada na *General Data Protection Regulation* (GDPR) aprovada pelo *Trialogue* da União Européia em 2015, representou um passo significativo ao reforçar a centralidade do consentimento no controle de dados pessoais[118] (Bioni, 2021). A GDPR reitera a necessidade de que o consentimento seja livre, específico, informado e inequívoco, deixando claro que esses qualificadores devem ser interpretados de forma cumulativa. Esse requisito busca assegurar que o consentimento

[116] Nesse contexto, destaca-se o princípio da proporcionalidade que cria a obrigação de o *data controller* não coletar dados excessivos diante do propósito especificado para o tratamento dos dados pessoais.
[117] A diretiva recorrentemente emprega o termo "*prior consent*" para estabelecer que, como regra, o controle sobre os dados pessoais deve ser exercido de forma prévia ao seu tratamento, e não posteriormente. Nesse sentido, consulte, por exemplo, os artigos 6(4), 8(3), 9(1) e 13(1).
[118] A GDPR busca proteger o direito à privacidade ao regular dados pessoais e sensíveis, ao mesmo tempo em que promove a circulação segura desses dados entre os Estados-membros da União Europeia, visando também ao fortalecimento da economia de dados (Custers, 2019).

corresponda de fato aos anseios do titular, seja manifestado por uma declaração ou por uma ação afirmativa clara, alinhada às expectativas de controle sobre os dados pessoais (Ramos, 2019).

Além disso, a GDPR refina ainda mais o tratamento do consentimento ao detalhar as condições que devem nortear a tomada de decisão do titular. Para isso, a norma determina que as informações fornecidas sejam claras, acessíveis e formuladas em linguagem simples, facilitando o entendimento do indivíduo sobre o uso de seus dados (Maldonado, 2020). O consentimento reafirma-se, assim, como um dos pilares da proteção de dados no contexto europeu, simbolizando o contínuo progresso das gerações legislativas voltadas à privacidade e ao controle informacional no ambiente digital (Bioni, 2021).

2.2.2.2 Formação e consolidação da legislação nacional sobre proteção de dados

Tendo em vista que até o ano de 2018[119] o Brasil não detinha legislação específica que tratasse sobre a proteção de dados pessoais, foi preciso harmonizar as mais diversas normas que mencionassem o tema para a aplicação da doutrina e jurisprudência, "com a finalidade de construir um sistema de proteção de dados que, nos termos da CF, proteja efetivamente a personalidade do cidadão" (MENDES, 2014, p. 141).

A Constituição Federal de 1988 representa o marco inicial[120] desse sistema de proteção, estabelecendo garantias como a inviolabilidade da vida privada e da intimidade (art. 5º, X), o sigilo das comunicações (art. 5º, XII) e o *habeas data*[121] (art. 5º, LXXII), que possibilita o acesso e a retificação de dados[122] (Doneda, 2015).

---

[119] Após anos de debates e sucessivos projetos de lei, a Lei nº 13.709, foi promulgada em 14 de agosto de 2018. A legislação entrou em vigor em 18 de setembro de 2020, com o objetivo de regulamentar o tratamento de dados pessoais no país, alinhando-se aos padrões internacionais de proteção de dados e buscando assegurar o direito à privacidade e à autodeterminação informativa dos cidadãos brasileiros.

[120] Ainda que o CC de 1916 já permitisse à doutrina brasileira o reconhecimento implícito dos direitos da personalidade, com base na interpretação de dispositivos que abordavam, de maneira indireta, aspectos extrapatrimoniais das relações sociais, a positivação expressa desses direitos fundamentais na CF de 1988 é um marco recente, resultado de uma evolução gradual e contínua (*Vide Capítulo 2.1.1.1*).

[121] A respeito da ação de *habeas data*, segundo Doneda (2020), a CF/1988 permitiu que os indivíduos pudessem ter acesso às suas informações colocadas em órgãos públicos, de modo a ser possível constatar certa influência da experiência europeia ou norte-americana relativa à proteção de dados pessoais já em pleno desenvolvimento à época (Doneda, 2020).

[122] Danilo Doneda (2011) destaca que, apenas no item 45 da Declaração de *Santa Cruz de La Sierra* (documento resultante da XIII *Cumbre Ibero-Americana* de Chefes de Estado e de Governo), assinada pelo Brasil em 15 de novembro de 2003, foi possível destacar uma primeira alusão expressa à proteção de dados pessoais em caráter de direito fundamental.

Seguindo essa linha evolutiva, a proteção dos dados pessoais foi gradualmente incorporada em normas subsequentes (Tasso, 2020). Um dos marcos importantes nesse percurso foi o Código de Defesa do Consumidor (CDC), Lei 8.078/1990, que ampliou a proteção de dados pessoais ao prever em seu artigo 43 o controle sobre todo e qualquer banco de dados e cadastro de consumidores que atinja o livre desenvolvimento da personalidade do consumidor[123] (Bioni, 2021).

Além disso, o artigo 43 do CDC estabelece obrigações aos gestores de bancos de dados, como a garantia de acesso às informações pelos consumidores (*caput*), a precisão dos dados armazenados (§3°), a limitação do uso dos dados a finalidades específicas e legítimas e a observância de um período máximo de cinco anos para a retenção de informações negativas (§1°). Essa regulamentação proporciona um sistema de proteção que visa à transparência e à responsabilidade, permitindo ao consumidor a possibilidade de corrigir ou excluir informações incorretas ou desatualizadas. Dessa forma, o CDC antecipa um modelo de proteção de dados que se orienta pela transparência[124] e pelo controle do titular, fortalecendo a autodeterminação informacional e estabelecendo uma base sólida para a proteção de dados pessoais no contexto brasileiro (Bioni, 2021).

No ano de 2011, foi promulgada a Lei 12.414/2011, conhecida como "Lei do Cadastro Positivo", que introduziu a obrigatoriedade do consentimento para o compartilhamento de dados financeiros e adimplentes dos consumidores para fins de concessão de crédito[125] (BIONI, 2021). Mendes (2011) argumenta que esta legislação marca a evolução do conceito de autodeterminação informativa no Brasil[126], ao exigir o consentimento explícito como condição para o tratamento de dados[127]. A Lei Complementar 166/2019, no entanto, retrocedeu para o sistema *opt-out*, permitindo a inclusão automática dos consumidores nos cadastros, conforme descreve Bioni (2021).

---

[123] Nesse sentido, Bioni (2021) destaca que a amplitude do dispositivo em questão alcança todo e qualquer dado pessoal do consumidor, indo muito além, portanto, dos bancos de dados de informações negativas para fins de concessão de crédito.

[124] A transparência exigida pelo CDC se fundamenta nos deveres atribuídos ao operador de bancos de dados: assegurar o acesso do consumidor às suas informações (art. 43, caput), garantir a precisão dos dados, limitar o uso a finalidades específicas e respeitar o prazo máximo de cinco anos para armazenamento de informações negativas (art. 43, § 1º).

[125] Tal definição pode ser extraída da interpretação conjunta dos arts. 1°, caput, 2°, III, e 3°, §1°.

[126] Sob esta perspectiva, Danilo Doneda (2015) argumenta que a Lei 12.414 de 2011, introduziu importantes princípios de proteção de dados pessoais no ordenamento jurídico brasileiro. Embora seu foco seja restrito ao contexto de históricos de crédito, essa legislação representou, à época, uma normativa que refletia de forma significativa um modelo de proteção de dados pessoais.

[127] Bioni (2021) aponta que esse sistema é reforçado pelo dever do gestor da base de dados de restringir a coleta de informações a dados essenciais, evitando incluir dados sensíveis, e utilizá-los unicamente para fins de análise de crédito.

Em 2014, foi promulgada a Lei 12.965/2014, conhecida como "Marco Civil da Internet" (MCI), estabelecendo uma normativa específica para os direitos e garantias dos cidadãos nas interações digitais. Entre os direitos assegurados, destacam-se a proteção da privacidade e dos dados pessoais[128], pilares do MCI ao lado da neutralidade de rede e da liberdade de expressão (Bioni, 2021).

A aprovação da lei foi impulsionada pelas denúncias de espionagem da Agência de Segurança Nacional dos Estados Unidos (NSA), reveladas por *Edward Snowden*[129]. Adotando uma abordagem principiológica, o MCI distanciou-se de legislações penais[130] que poderiam restringir o desenvolvimento tecnológico, como explica Bioni (2021). Embora mencionasse o consentimento e suas qualificações[131], o MCI não abordava diretamente a proteção de dados, uma lacuna preenchida pela LGPD em 2018.

A LGPD introduziu uma regulamentação mais abrangente para a proteção de dados no cenário jurídico nacional. Fortemente influenciada pela GDPR da União Europeia (*Vide Capítulo 2.2.2.1*), ambas compartilham conceitos e diretrizes similares[132] (Lorenzon, 2021). Desde 2010, discutia-se no Brasil a necessidade de uma legislação específica para proteger os dados pessoais.

A primeira versão do anteprojeto da LGPD, conforme Bioni (2021), estabelecia o consentimento como a única base para o tratamento de dados. Contudo, após consultas públicas,

---

[128]O MCI não é um documento normativo específico sobre privacidade e proteção de dados, mas trata dessa temática em alguns dos seus artigos (Ferreira; Pinheiro; Marques, 2021). Veja, nesse sentido: Art. 3°, II e III, do MCI: "A disciplina do uso da *internet* no Brasil tem os seguintes princípios: (...) II –proteção da privacidade; III – proteção dos dados pessoais, na forma da lei".

[129] O jornal britânico *The Guardian* publicou, com exclusividade, uma série de reportagens assinadas por Glenn Greenwald (2013) sobre os programas de espionagem da Agência de Segurança Nacional dos EUA (NSA). A NSA monitorou dados de ligações telefônicas de cidadãos americanos, além de coletar fotos, *e-mails* e videoconferências de usuários de serviços *online* oferecidos por empresas como *Google*, *Facebook* e *Microsoft/Skype*. Posteriormente, o jornal revelou que Edward Snowden, ex-funcionário de uma prestadora de serviços da NSA, era a fonte das informações. Snowden expôs o sistema de vigilância secreto *XKeyscore*, que permitia à inteligência americana monitorar a atividade de usuários de *internet* ao redor do mundo (Greenwald, 2013).

[130] Mais precisamente, o MCI surgiu como uma alternativa à chamada 'Lei Azeredo', projeto de lei que propunha o estabelecimento de uma ampla legislação criminal para a *internet*, e assim batizada por conta do seu relator e mais assíduo defensor, o deputado Eduardo Azeredo (PSDB-MG). A percepção de um amplo espectro da sociedade brasileira é que a Lei Azeredo, se aprovada, provocaria um grande retrocesso no ambiente regulatório da *internet* no país (Lemos 2014)

[131] Art. 7º, VI, VIII, IX e XI, do MCI: "o acesso à *internet* no Brasil assegura ao usuário os seguintes direitos: (...) VI – consentimento livre, expresso e informado para coleta, uso, armazenamento e tratamento de dados pessoais; VIII – exclusão definitiva dos dados pessoais que tiver fornecido a determinado serviço de *internet*, mediante solicitação; IX – informação clara e completa sobre coleta, uso, armazenamento e tratamento de seus dados, que só poderão ser utilizados para finalidades que justifiquem sua coleta; XI – fornecimento a terceiros apenas nas hipóteses previstas em lei ou com o consentimento do usuário."

[132] A LGPD, similar à GDPR, introduz conceitos fundamentais como "dados pessoais", "dados pessoais sensíveis", "anonimização de dados" e "tratamento de dados" (Lorenzon, 2021), alinhando suas diretrizes com o padrão europeu para proteger direitos individuais na coleta e uso de informações pessoais.

o anteprojeto foi significativamente revisado, resultando em uma estrutura que posiciona o consentimento como uma entre várias bases legais para o tratamento de dados, listadas de forma horizontal e sem hierarquia no art. 7°. Essa mudança reflete uma abordagem mais flexível, permitindo que outras bases legais sejam utilizadas para o tratamento de dados, de acordo com diferentes contextos (Bioni, 2021).

Apesar da inclusão de múltiplas bases legais, o consentimento continua sendo um elemento central na LGPD, mencionado 35 vezes ao longo do texto legal (Lugati; De Almeida, 2020). Nesse contexto, Bruno Ricardo Bioni (2021, p. 131-132) observa que uma análise aprofundada do corpo normativo da LGPD revela uma preocupação evidente com a participação ativa do indivíduo no controle de suas informações pessoais:

> Primeiro, por adjetivar extensivamente o consentimento seguindo a linha evolutiva do direito comunitário europeu e da quarta geração de leis de proteção de dados pessoais. (...) Segundo, porque grande parte dos princípios tem todo o seu centro gravitacional no indivíduo. (...) Terceiro, porque há uma série de disposições que dão um regramento específico para concretizar, orientar e, em última análise, reforçar o controle dos dados pessoais por meio do consentimento.

Esses requisitos sublinham o papel fundamental do consentimento na LGPD, reforçando a ênfase normativa na autonomia informacional do titular e na transparência no tratamento de dados (Bioni, 2021).

2.3 ASSIMETRIA INFORMACIONAL E A FRAGILIDADE DO CONSENTIMENTO COMO FOCO REGULATÓRIO

Conforme argumenta Daniela Toniazzo (2022), a LGPD estabelece que o tratamento de dados não pode ser realizado sem uma fundamentação normativa que o autorize, e, sendo o consentimento o suporte escolhido, ele deve estar dotado das características referidas na Lei

para ser válido[133], sob pena de violação à legislação protetiva de dados[134]. Assim, o consentimento precisa ser livre, informado e inequívoco, como especificado no artigo 5º, XII, da LGPD. Essas características são essenciais para assegurar que a autorização para o tratamento de dados represente, de fato, uma expressão autêntica de autodeterminação informativa, e não uma mera formalidade.

Em um contexto em que "você é a mercadoria" (*Vide Capítulo 1.2.2.1*), de ostensiva produção de "superávits comportamentais" (*Vide Capítulo 1.2.2*) – insumos de uma economia preditiva alicerçada na extração e no processamento cada vez maior e mais efetivo de dados como consequência ao *machine learning*[135] e ao *big data* – e de frágeis mecanismos jurídicos operacionalizadores do consentimento, (Bioni, 2021), o confronto com situações reais revela que, em tais situações, a opção por não consentir à cessão dos dados pessoais pelo seu titular tende a ser uma renúncia a determinados bens ou serviços (Doneda, 2020). Nesse sentido complementa Danilo Doneda (2020, p. 293):"a disparidade de meios e de poder entre a pessoa de quem é demandado o consentimento para utilização dos dados pessoais em contemplação da realização de um contrato e aquele que os pede faz com que a verdadeira opção que lhe reste seja, tantas vezes, a de 'tudo ou nada', 'pegar ou largar'".

Veja, nesse sentido, que o progresso geracional de leis de proteção de dados, falhou ao preocupar-se excessivamente com a adjetivação do consentimento em detrimento de sua

---

[133] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiros; III - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

[134] Segundo Bioni (2021), o consentimento, no direito privado brasileiro, tem sido tradicionalmente analisado sob a perspectiva dos defeitos do negócio jurídico. Nesse contexto, garantir que a declaração de vontade seja "livre e consciente" é o bem jurídico tutelado. Quando esse elemento volitivo se forma de maneira imperfeita, caracteriza-se o "vício de consentimento", tornando o negócio jurídico resultante passível de anulação.

[135] Segundo Domingos (2017), enquanto os algoritmos convencionais recebem dados como entrada e produzem um resultado, o *machine learning* inverte essa lógica: ele recebe os dados juntamente com o resultado desejado e gera um algoritmo capaz de transformar os primeiros no segundo. Assim, os algoritmos de aprendizado, conhecidos como aprendizes, são responsáveis pela criação de outros algoritmos, permitindo que os computadores desenvolvam seus próprios programas, eliminando a necessidade de programá-los diretamente. Nesse sentido, quanto mais dados alimentam o *machine learning*, maior a sua capacidade de processamento e precisão.

operacionalização, o que abriu margem para que os agentes de processamento estabelecessem unilateralmente os contratos que regulam a relação jurídica entre as partes (Bioni, 2021).

Portanto, como argumenta Stefano Rodotà (2008), diante do "pegar ou largar" do "aceite" – ou, *click-wrap*[136] – às regras de adesão[137], sua anuência implica na obrigação do indivíduo "a expor seu próprio eu, sua própria *persona*, com consequências que vão além da simples operação econômica e criam uma espécie de posse permanente da pessoa por parte de quem detém as informações a seu respeito" (Rodotà, 2008, p. 113).

Diante desse diagnóstico, percebe-se que ao alocar o consentimento como sendo o eixo gravitacional da disciplina, o interessado somente poderá alcançar a tutela em um momento posterior ao consentimento, valendo-se da arguição de algum defeito deste – uma vez que a pessoa teria que primeiro, concordar em ceder seus dados para somente depois se valer da tutela do que foi cedido (Doneda, 2020). Laura Schertel Mendes e Gabriel da Fonseca (2020, p. 513-519) elencam três pontos que elucidam as insuficiências do foco regulatório no consentimento:

> (i) as limitações cognitivas do titular dos dados pessoais para avaliar os custos e benefícios envolvidos quanto aos seus direitos de personalidade; (ii) as situações em que não há uma real liberdade de escolha do titular como, por exemplo, em circunstâncias denominadas de "*take it or leave it*"; e (iii) as modernas técnicas de tratamento e análise de dados a partir de *big data* que fazem com que a totalidade do valor e a possibilidade de uso desses dados não sejam completamente mensuráveis no momento em que o consentimento é requerido.

Sendo assim, a assimetria informacional entre os "polos" dessa relação se manifesta como um fenômeno multidimensional que impõe uma sobreposição de fragilidades, na medida em que o sujeito se (hiper)vulnerabiliza ao ser inserido em um novo contexto: o mercado informacional (Bioni, 2021).

No entanto, muito embora se dedique um diploma próprio para tratar dessa situação específica de vulnerabilidade na LGPD[138], percebe-se uma incompatibilidade do arranjo

---

[136] De acordo com Cíntia de Lima (2014), para que ocorra o aceite em contratos na *internet*, é necessário que o usuário se identifique pessoalmente e clique no ícone indicando sua concordância, geralmente com a expressão "li e aceito os termos e condições de uso", prática conhecida como *click-wrap*. O contrato *click-wrap* é um tipo de contrato de adesão telemático, cujo objeto pode ser um bem digitalizado ou material, por meio do qual o fornecedor define unilateralmente as cláusulas contratuais e as notifica ao usuário antes de obter seu consentimento, que é manifestado por meio de um clique.

[137] Segundo Silvio Rodrigues (2004), um contrato de adesão é caracterizado por ter todas as cláusulas previamente estabelecidas por uma das partes, deixando a outra, geralmente a parte mais vulnerável e necessitada do contrato, sem possibilidade de discutir ou alterar as condições. A essa parte resta apenas a opção de aceitar ou rejeitar o contrato em sua totalidade.

[138] Veja nesse sentido o capítulo II da LGPD, em especial as seções I, II e III, que tratam respectivamente dos requisitos para o tratamento de dados pessoais; do tratamento de dados pessoais sensíveis e do tratamento de dados pessoais de crianças e adolescentes.

normativo em reconhecer essa (hiper)vulnerabilidade ao "apostar todas as fichas normativas" no consentimento, como se a parte mais fraca desse arranjo regulatório fosse um sujeito racional, livre, capaz para fazer valer a proteção de seus dados pessoais (Bioni, 2021).

2.3.1 A complexidade do fluxo informacional e as limitações para um genuíno processo de tomada de decisão

O avanço das tecnologias de *big data* e *machine learning* tem intensificado os desafios relacionados à proteção de dados, especialmente no âmbito do consentimento. Segundo Bruno Ricardo Bioni (2021), a complexidade intrínseca aos fluxos informacionais cria barreiras cognitivas que comprometem significativamente a capacidade do indivíduo comum de exercer controle efetivo sobre suas informações pessoais[139].

Para Laura Schertel Mendes e Gabriel da Fonseca (2020) a ênfase excessiva na obtenção do consentimento informado negligencia um aspecto mais complexo: a efetiva capacidade do titular dos dados pessoais de compreender e avaliar, de forma substancial, os riscos e potenciais prejuízos decorrentes de seu consentimento, especialmente no ambiente *online*. Nesse sentido, complementam os autores (2020, p. 515):

> Apesar da grande relevância dada à apresentação de informações pela entidade responsável pelo tratamento de dados, estudos têm indicado que, ao tomar decisões sobre sua privacidade e sobre seus dados, os indivíduos muitas vezes sequer leem regularmente as "Políticas de Privacidade" ou "Informações sobre o Uso de Dados" que lhe são apresentadas, o que pode tornar a medida inócua. Mais do que isso, as informações disponibilizadas costumam ser de difícil compreensão, haja vista a complexidade e sofisticação do tratamento de dados na espécie, envolvendo vários conceitos técnicos e jurídicos ou até mesmo o tamanho das letras e a extensão do texto. Em verdade, o próprio excesso de informações pode ser prejudicial, sobrecarregando a cognição do titular dos dados acerca dos efeitos atinentes às questões apresentadas. Além disso, até mesmo a maneira com que essas regras e essas escolhas são disponibilizadas (*framed*) pode influenciar sensivelmente o processo decisório de se consentir ou não.

A opacidade dos instrumentos operacionalizantes impede que o consentimento seja verdadeiramente informado, visto que os titulares de dados não têm clareza sobre o que está

[139] Conforme explica o autor, essa limitação decorre da racionalidade limitada do ser humano, que torna improvável a capacidade dos indivíduos de avaliar de forma abrangente os benefícios e riscos associados ao consentimento para o processamento de seus dados. Esse conceito, denominado "*bounded rationality"*, refere-se à incapacidade humana de absorver, reter e processar todas as informações relevantes para uma tomada de decisão plenamente informada e legítima (Bioni, 2021).

sendo coletado, como seus dados serão processados ou reutilizados nem quais são os riscos envolvidos (Nissenbaum; Barrocas, 2009).

Igualmente, o consentimento na forma como é atualmente operacionalizado tem estrangulado a liberdade de escolha do titular ao impor a lógica do "*take it or leave it*"[140], na qual ou o titular aceita a coleta dos seus dados ou é impedido de utilizar determinada aplicação ou serviço (*Vide Capítulo 2.3*) (Mendes; Da Fonseca, 2020).

De igual maneira, o uso de algoritmos e decisões automatizadas – *machine learning* – introduzem um nível de complexidade significativo no fluxo de informações (Monteiro, 2018). Esses algoritmos ao se adaptarem às variáveis de entrada (*input*), podem produzir novos dados (*output*) que afetem significativamente a vida dos usuários (*Vide Capítulo .1.2*). Todavia, essa adaptabilidade também resulta na falta de clareza sobre a lógica por trás do tratamento de dados, dificultando a verificação de sua legitimidade, proporcionalidade e "finalidade esperada"[141] (*Ibidem*). Isso compromete o "direito à explicação", essencial para que os titulares entendam o uso de seus dados em decisões, como concessão de crédito. Tanto a LGPD[142] quanto o GDPR[143] abordam esse problema, oferecendo o direito à revisão de decisões automatizadas, mas a aplicação desse direito enfrenta desafios práticos.

Para Marion Albers (2016), a complexidade do fluxo informativo no contexto da "sociedade da informação", exige uma regulamentação igualmente complexa e de múltiplos níveis, que considere não apenas os dados em si, mas todo o fluxo de informações e decisões que deles derivam. A complexidade intrínseca ao fluxo de dados modernos exige que a regulamentação vá além da simples coleta de consentimento e inclua mecanismos robustos de transparência, explicação e responsabilidade dos agentes de tratamento de dados (Albers, 2016). Assim, torna-se evidente que o consentimento, isoladamente, não é suficiente para lidar com os desafios contemporâneos de proteção de dados e é necessário integrá-lo com outros

[140] "Pegar ou largar" em tradução livre.

[141] O Princípio da Finalidade está previsto no artigo 6º, inciso I, da LGPD. Ele determina que o tratamento de dados pessoais deve ter um propósito específico e legítimo, previamente informado ao titular. Isso impede o uso de dados para finalidades diferentes das informadas inicialmente, evitando abusos e garantindo maior transparência. Por exemplo, dados coletados para cadastro não podem ser repassados a terceiros para outros usos sem o consentimento do titular.

[142] Na LGPD brasileira, o direito à revisão de decisões automatizadas está previsto no artigo 20, que estabelece que o titular dos dados tem o direito de solicitar a revisão de decisões tomadas exclusivamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluindo decisões destinadas a definir seu perfil pessoal, profissional, de consumo e de crédito ou aspectos de sua personalidade.

[143] No GDPR da União Europeia, esse direito é contemplado no artigo 22, que dispõe sobre a proibição de decisões automatizadas com efeitos legais ou significativos sobre o indivíduo, salvo em situações específicas, como quando há consentimento explícito, necessidade para execução de um contrato ou autorização legal, assegurando, nesses casos, o direito à revisão humana, à explicação e à contestação.

instrumentos regulatórios que garantam uma proteção efetiva aos direitos fundamentais dos indivíduos (Albers, 2016).

Portanto, para que o consentimento seja genuíno e eficaz no ambiente informacional contemporâneo, é necessário repensar o seu papel e os mecanismos de suporte. Como observado por Mendes e Fonseca (2020), a introdução de estratégias como a proteção de dados por *design*, por padrão, *accountability*[144] e limitações contextuais ao consentimento são fundamentais para garantir que o titular tenha um verdadeiro controle sobre suas informações. Sem essas inovações, o consentimento continuará a ser um mecanismo insuficiente para lidar com a complexidade do fluxo de dados e com as decisões automatizadas que impactam diretamente a vida dos indivíduos.

2.3.2. A hipervulnerabilidade do usuário

A era digital trouxe inúmeras facilidades, mas também criou um ambiente propício à exploração dos dados pessoais, exacerbando a vulnerabilidade dos usuários (Siqueira *et al.*, 2021). O conceito de vulnerabilidade, que tradicionalmente se aplicava às relações de consumo[145], expande-se ao ambiente digital para englobar a lógica própria dessa relação de consumo (Bioni, 2021).

Diante da complexidade do fluxo informacional e das limitações do indivíduo para um genuíno processo de tomada de decisão (*Vide Capítulo 2.3.2.1*), percebe-se um traço vulnerante peculiar sob diversas perspectivas: informacional, técnica e econômica (Bioni, 2021). Portanto, diante da sobreposição de fraquezas, os indivíduos são considerados hipervulneráveis na medida em que aceitam tudo aquilo que lhes é imposto nas contratações (Góes*et al*, 2021). Nesse sentido, Bruno Bioni (2021, p. 144) complementa:

> O ser humano tem a tendência de focar nos benefícios imediatos, o que, de acordo com o arranjo e os modelos de negócios da economia informacional, é representado pelo acesso a um produto ou serviço *online*. Por tal razão, deixa de sopesar os

[144] Sem esgotar as hipóteses, que serão tratadas em capítulo futuro, a *accountability* promove a proteção de dados por meio de um sistema robusto de prestação de contas pelos agentes de tratamento, conforme o entendimento de Mendes e Fonseca (2021). Esse sistema é apto a identificar e dimensionar os riscos prévios ao tratamento de dados pessoais, exigindo que as organizações não apenas sigam as normas de proteção, mas também comprovem sua conformidade.

[145] Para Bioni (2021), o direito do consumidor nasce ideologicamente com o objetivo de corrigir a desigualdade entre consumidores e prestadores ou fornecedores de produtos e serviços. Nesse sentido, o direito do consumidor visa a proteger o elo mais frágil da cadeia econômica, que tende a se submeter ao poder de controle dos detentores dos bens de produção. A partir disso, surge a noção de instrumentalidade do direito, que fundamenta a criação de normas protetivas para garantir um tratamento desigual entre sujeitos desiguais.

> possíveis prejuízos à privacidade, que são temporariamente distantes. De fato, os possíveis danos com relação à perda do controle sobre as informações pessoais só podem ser experimentados no futuro.

Em um contexto em que os dados pessoais se tornaram o principal ativo de uma nova economia (*Vide Capítulo 1.2.2.1*), o indivíduo se encontra em uma posição de extrema desvantagem. Contudo, a hipervulnerabilidade do indivíduo não se limita à exploração comercial de dados, uma vez que, o ambiente digital também é um terreno fértil para a prática de crimes cibernéticos[146], que exploram a falta de conhecimento técnico dos usuários (Siqueira*et al*, 2021). Muitos consumidores não têm plena consciência dos riscos que enfrentam ao compartilhar suas informações pessoais, tornando-se frequentemente alvos de golpes e fraudes digitais.

Portanto, a hipervulnerabilidade do usuário no ambiente digital não é apenas uma questão de falta de controle sobre os dados, mas também de como esse ambiente é estruturado para maximizar a exploração dessas informações (Bioni, 2021). Nesse contexto, em vez de simplesmente assegurar artificialmente múltiplos qualificadores para o consentimento, torna-se imperativo buscar, prioritariamente, outras estratégias regulatórias que visem a mitigar a assimetria informacional identificada, reconfigurando, assim, sua dinâmica de poder[147] (Bioni, 2021).

[146] Os crimes cibernéticos ou crimes de informática podem ser classificados como condutas que atentam contra dados e contra o computador (e através dele), ou seja, são aqueles "crimes relacionados às informações arquivadas ou em trânsito por computador, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico" (Corrêa, 1999, p. 43).

[147] Para Lucas de Souza Lehfeld (2021), os dados pessoais devem ser compreendidos não apenas como uma fonte de riqueza, mas, principalmente, como uma fonte de poder, especialmente no que se refere ao controle da sociedade. Dessa forma, diante da ausência de proteção adequada aos consumidores *online*, a *internet* configura-se como um potencial meio para a violação de direitos fundamentais.

CAPÍTULO 3 – AUTODETERMINAÇÃO INFORMACIONAL VS REGULAÇÃO DO RISCO: UMA ABORDAGEM SISTÊMICA DA LEI GERAL DE PROTEÇÃO DE DADOS

3.1 UM DIAGNÓSTICO DE ASSIMETRIAS PARA UM CONTROLE MAIS EFETIVO DOS DADOS PESSOAIS

> Atrás de Winston, a voz da teletela continuava balbuciando sobre o ferro-gusa e a superação das metas do Nono Plano Trienal. A teletela recebia e transmitia informação ao mesmo tempo. Qualquer som que Winston emitisse, para além de um sussurro baixíssimo, era captado pelo aparelho; e enquanto permanecesse dentro do campo de visão controlado pela placa de metal, podia ser visto e ouvido. Ninguém sabia, é claro, quando estava sendo vigiado. Também não se sabia ao certo com que frequência a Polícia do Pensamento se conectava a um aparelho específico, nem como funcionava esse sistema. Era possível, inclusive, que vigiasse a todos o tempo todo. De um jeito ou de outro, podiam se conectar a qualquer aparelho quando bem quisessem. As pessoas tinham que viver - e viviam, primeiro por hábito e depois por instinto - sob a hipótese de que todo som emitido era ouvido e de que, exceto no escuro, todo movimento era perscrutado (ORWELL, 2021, p. 22).

Não raramente associam[148] o acesso indiscriminado aos nossos dados pessoais com a vigilância operada pela "teletela *orwelliana*" centralizada na figura do "*Big Brother*" no romance intitulado "1984" de Eric Arthur Blair[149]. Embora essa analogia seja válida para compreender cenários de monitoramento social, a "sociedade da informação" introduziu desafios novos e significativamente mais complexos, que nos distanciam em diversos aspectos da realidade ficcional descrita na obra.

Na narrativa de George Orwell, o protagonista Winston apresenta a Oceania, um Estado distópico em que a vigilância ostensiva é utilizada como instrumento para intimidar e controlar os cidadãos. Esse monitoramento é conduzido pelo aparato estatal, simbolizado pela "teletela" e personificado na figura do "*Big Brother*", cuja principal função é assegurar a obediência e a submissão da população ao regime autoritário.

No entanto, a "sociedade da informação" ressignificou e ampliou o conceito de vigilância, distanciando-se da definição clássica apresentada em "1984". Nesse novo contexto, a vigilância deixa de ser um fenômeno estanque e hierárquico, caracterizado por uma relação fixa entre observador e observado, para assumir formas descentralizadas e dinâmicas. O ato de vigiar, antes concentrado em figuras homogêneas como o "*Big Brother*" e na tecnologia

[148] Veja nesse sentido: Bruno Bioni (2021, p. 137-142), Danilo Doneda (2020, p. 36), Laura Schertel Mendes (2008, p. 75), Stefano Rodotà (2008, p. 25) e Helen Nissenbaum (2010, p. 93).
[149] Esse era o nome real do romancista, sendo George Orwell o pseudônimo que utilizava.

centralizada da "teletela", se expande em um movimento plural e descentralizado, caracterizado pela multiplicidade de observadores e pela disseminação de inúmeras tecnologias voltadas a esse propósito (*Vide Capítulo 2.1.2.2*) (Bioni, 2021).

A “sociedade da informação” introduziu novos desafios à proteção de dados. Diferentemente do romance “1984”, a pessoa de carne e osso está em contínuo estado de visibilidade e sujeita a uma vigilância mais opaca, dispersa, extensiva e intensiva (Bioni, 2021), intensificando assimetrias (*Vide Capítulo 2.3.1*) e (hiper)vulnerabilidades (*Vide Capítulo 2.3.2*).

Nesse contexto, a história demonstra esforços para equalizar essas assimetrias por meio de regulamentações específicas destinadas a mitigar vulnerabilidades emergentes em cada período histórico (*Vide Capítulo 2.2.1*).O avanço das legislações de proteção de dados consolidou a autodeterminação informativa como o principal mecanismo de proteção do indivíduo, estabelecendo o consentimento como pilar central dessa estratégia regulatória.

No entanto, a estratégia regulatória, embora tenha atribuído ao consentimento diversas qualificações — como inequívoco, expresso, informado, específico ou livre (Bioni, 2021) —, falhou em dedicar atenção proporcional à forma como esse consentimento deveria ser efetivamente operacionalizado.

3.1.1 As fragibilidades do atual modelo de contratação do consentimento

O surgimento da *internet* como um espaço global de interação e comunicação provocou intensos debates sobre as possibilidades e os limites da regulação do ciberespaço[150]. No final dos anos 1990 e início dos anos 2000, prevaleceu a percepção de que a *internet* seria um ambiente de igualdade universal, caracterizado por sua natureza descentralizada e pela ausência de hierarquias coercitivas tradicionais (Carvalho; Negócio, 2023). Esse entendimento foi reforçado por desafios éticos e materiais: a ausência de legitimidade das estruturas estatais no domínio virtual e a complexidade técnica que dificultava a regulação governamental direta

[150] Nesse sentido, é importante compreender que a regulamentação da *internet* e a regulamentação da proteção de dados pessoais possuem finalidades, abrangências e normas distintas. Enquanto a regulamentação da *internet* se concentra em aspectos como o acesso à rede, neutralidade, segurança cibernética, direitos digitais e responsabilidade de provedores, a proteção de dados pessoais é focada na privacidade, segurança e tratamento adequado das informações pessoais coletadas, armazenadas e compartilhadas por empresas, organizações e instituições públicas. Embora possam se relacionar em determinados contextos, cada área possui diretrizes específicas que atendem a diferentes objetivos e públicos.

sobre esse novo meio[151] (Silva, 2022). Esses fatores impulsionaram a adoção de modelos de autorregulação como alternativa normativa predominante no ambiente digital.

A autorregulação, conforme definida por Carolina Borges (2024), constitui uma manifestação específica da regulação, caracterizada pela ausência de intervenção estatal direta. Nesse modelo, indivíduos e entidades privadas estabelecem padrões regulatórios públicos e formalizados para a condução de suas atividades. Esse princípio tornou-se fundamental no ambiente digital, especialmente diante da lacuna normativa deixada pela ausência de regulação estatal abrangente (Carvalho; Negócio, 2023). Nesse contexto, as plataformas digitais não apenas implementaram normas internas, mas também desenvolveram arquiteturas tecnológicas que condicionam e limitam as ações de seus usuários.

O surgimento dos termos de uso e políticas de privacidade[152] são consequência dessa demanda regulatória. Esses instrumentos, concebidos como mecanismos de autorregulação, emergiram, em um primeiro momento, como expressão da lógica da "sociedade da informação", na qual a coleta e o processamento de dados pessoais se consolidaram como pilares do modelo econômico, assegurando a liberdade conveniente para a sua operação (De Araújo; Carvalheiro, 2014). Em um segundo momento, tornaram-se uma resposta ao descompasso normativo gerado pelo progresso geracional das legislações de proteção de dados pessoais. Esse arcabouço jurídico enfatizou a adjetivação do consentimento em detrimento de sua operacionalização, delegando a ele a tarefa de equilibrar as assimetrias (*Vide Capítulo 2.3*) existentes na relação entre usuário e provedor. Contudo, tal abordagem resultou em novas vulnerabilidades (*Vide Capítulo 2.3.2.*), especialmente no que tange à autodeterminação informacional (Bioni, 2021).

---

[151] Conforme Rosane L. da Silva (2010, p. 3909), o uso das tecnologias da informação e comunicação trouxe à tona novos conflitos, marcados por questões técnicas alheias ao universo jurídico. Esse cenário revelou a ausência de respostas prontas no aparato normativo e a dificuldade de regulamentar matérias dinâmicas, como a proteção de dados pessoais na *internet*. Em razão disso, nos primeiros anos de utilização da rede mundial de computadores, houve uma proliferação de códigos deontológicos, políticas de boa conduta e políticas de privacidade e segurança, amplamente divulgadas nos sites das empresas atuantes nesse setor.

[152] As nomenclaturas atribuídas a documentos regulatórios no ambiente digital podem variar, refletindo a diversidade de abordagens normativas adotadas por plataformas e entidades privadas. Entre os principais exemplos, destacam-se os "Termos de Uso e a Política de Privacidade", que funcionam como contratos estabelecendo os direitos e deveres das partes. Outras denominações comuns incluem "Política de *Cookies*", "Termos e Condições", "Política de Reembolso" e "Aviso Legal", além de variações como "Diretrizes de Uso", "Código de Conduta" e "Contrato de Adesão".

Essas “regras de conduta ou normas-padrão”, em sua essência, representam contratos de adesão[153], por meio de que os indivíduos são colocados diante de escolhas ilusórias[154], resumidas no modelo "*take it or leave it*" (Mendes; Da Fonseca, 2020). Como apontado por Bioni (2021), esses instrumentos muitas vezes transferem aos usuários a responsabilidade de compreender e gerenciar riscos complexos associados ao uso de seus dados, mesmo diante de assimetrias informacionais evidentes e da opacidade técnica inerente às plataformas digitais (*Vide Capítulo 2.3.1*).

A ênfase no consentimento como pilar central da proteção de dados, embora normativa e teoricamente robusta, revelou-se insuficiente em termos práticos (Lugati; De Almeida, 2020). Estudos de Daniel J. Solove (2013) destacam que o consentimento raramente é significativo, dada a dificuldade dos indivíduos em compreender as implicações de suas escolhas em um cenário marcado pela coleta massiva e pela análise preditiva de dados. Além disso, a fragmentação dos processos de vigilância digital, característica da “sociedade da informação”, dificulta a operacionalização do controle individual sobre os dados compartilhados.

A introdução de legislações como o MCI e a LGPD buscou corrigir essas insuficiências, promovendo uma regulação da autorregulação[155], a partir de que a responsabilidade das plataformas é ampliada pela imposição de requisitos como a transparência, finalidade, segurança e prestação de contas (MAGRO, 2020). Entretanto, mesmo sob essa nova configuração, os desafios persistem. A LGPD, por exemplo, incorpora princípios como o

[153] Neste trabalho, adotou-se o entendimento de que as políticas de privacidade se configuram como "contratos de adesão", em conformidade com a doutrina de Orlando Gomes (1972, p. 05-09). Todavia, uma parcela da doutrina as classifica como "condições gerais de contratação". Nesse sentido, ver Cláudia L. Marques (2011, p. 74-75; 86-87).

[154] As políticas de privacidade, aqui classificadas como "contratos de adesão", revelam uma capacidade ilusória de escolha por parte do sujeito aderente. Essa ilusão decorre de dois fatores principais: a complexidade e abstração dos termos, que dificultam uma compreensão transparente sobre o uso concreto dos dados, e a imposição de uma lógica binária de adesão ("*take it or leave it*"), na qual o consentimento é apresentado como condição indispensável para o acesso ao serviço desejado, como redes sociais ou aplicativos online. Assim, a ausência de consentimento implica, invariavelmente, a exclusão do sujeito do uso do serviço, evidenciando o caráter coercitivo subjacente à decisão formalmente voluntária (Balkin, 2018, p. 3).

[155] A autorregulação regulada constitui um modelo híbrido de regulação em que o Estado exerce influência direta sobre os sistemas autorregulatórios, com o objetivo de assegurar que os atores privados atuem em conformidade com interesses coletivos e o bem comum. Nesse arranjo, combina-se a autonomia normativa do setor privado com a supervisão estatal, promovendo um equilíbrio entre a liberdade regulatória das empresas e a proteção dos direitos dos usuários e consumidores. Como descrito por Américo R. Magro (2020, p. 42), essa abordagem busca mitigar abusos e desigualdades inerentes ao modelo de autorregulação pura, estabelecendo uma integração entre os sistemas normativos de direito público e privado. Assim, o Estado desempenha um papel de mediador, garantindo que os mecanismos autorregulatórios sejam utilizados de forma responsável e orientada por valores éticos e sociais (Hoffman-Riem, 2019, p. 547).

"*privacy by design*"[156] e a "*accountability*"[157], que representam avanços regulatórios significativos. O primeiro princípio exige que a proteção de dados seja integrada desde a concepção de produtos e serviços, mitigando os riscos potenciais por meio da adoção de soluções tecnológicas preventivas. Já a *accountability* estabelece um modelo de responsabilização que demanda que os agentes de tratamento demonstrem conformidade ativa com as normas de proteção de dados, incluindo a documentação de procedimentos, avaliações de impacto e a implementação de boas práticas para garantir a segurança e privacidade dos dados pessoais (Bioni; Zanatta, 2020). Contudo, a execução efetiva dessas medidas ainda enfrenta barreiras técnicas e práticas, como a dificuldade de auditar algoritmos e a resistência das corporações em implementar mudanças estruturais (De Souza, 2024).

Além disso, como discutido por Prazeres (2022), a sociedade contemporânea está imersa em uma dinâmica de capitalismo de vigilância, em que o comportamento humano é transformado em mercadoria. Nesse contexto, as políticas de privacidade não apenas falham em proteger a autodeterminação informacional, mas também reforçam desigualdades estruturais ao atribuírem excessiva importância ao instituto do consentimento. Há, assim, uma "hipertrofia" desse mecanismo, que não consegue acompanhar a complexidade dos fluxos informacionais no ambiente digital (Bioni, 2021). Portanto, é necessário repensar a autodeterminação informativa para além da lógica binária de consentir ou não com o tratamento de dados pessoais, exigindo uma tutela jurídica que ultrapasse esse raciocínio simplista e considere as nuances de um cenário de vigilância descentralizada (Lugati; De Almeida, 2020).

Nesse sentido, o consentimento enfrenta desafios práticos e conceituais em um contexto de disseminação massiva de dados, em que os termos de uso e políticas de privacidade operam como contratos de adesão obrigatórios. Estudos, como o realizado pela Universidade de Stanford (Romero, 2017), demonstram que 97% dos usuários não leem os termos de uso e políticas de privacidade antes de concordar com eles, evidenciando que o "clique no eu aceito" raramente reflete uma manifestação de vontade consciente e informada. Essa prática, por sua vez, expõe a fragilidade do consentimento como instrumento jurídico no contexto digital, uma

[156] O artigo 46 da LGPD determina que os agentes de tratamento de dados devem implementar medidas de segurança, tanto técnicas quanto administrativas, para proteger os dados pessoais contra acessos não autorizados, além de prevenir destruição, perda, alteração ou comunicação inadequada, seja por ações acidentais ou ilícitas. O § 2º reforça a obrigatoriedade de que essas medidas sejam aplicadas desde a fase de concepção até a execução de produtos ou serviços, alinhando-se ao princípio do "*privacy by design*".

[157] O artigo 6º, inciso X, da LGPD estabelece o princípio da responsabilização e prestação de contas, que exige dos agentes de tratamento a demonstração da adoção de medidas eficazes para assegurar a conformidade com as normas de proteção de dados pessoais. Além disso, o agente deve ser capaz de comprovar a eficácia dessas medidas, promovendo transparência e garantindo a accountability no tratamento de dados.

vez que a recusa em aceitar tais termos frequentemente resulta na exclusão social e digital, considerando que a inserção e a participação ativa na sociedade contemporânea são intrinsecamente dependentes do trânsito informacional (Doneda, 2020). Conforme argumenta Bioni (2021), o indivíduo, posicionado como elo mais vulnerável na relação com grandes plataformas, é constrangido a aderir às dinâmicas de mercado, enfrentando escolhas ilusórias que inviabilizam decisões plenamente racionais. Tal cenário é amplificado por estratégias de *big data* e mecanismos de publicidade persuasiva, que moldam comportamentos e intensificam as assimetrias de poder entre usuários e provedores de serviços digitais (*Vide Capítulo 2.1.2.3*).

3.1.1.1 Cookies, entre facilidades e desafios.

Os *cookies*, pequenos arquivos de texto armazenados pelo navegador (*web browser*), desempenham um papel central na dinâmica da coleta de dados na *internet* (Souza, 2018, p. 26). Originalmente concebidos para otimizar a navegação, facilitar a funcionalidade de *websites* e personalizar experiências, eles se tornaram ferramentas poderosas para rastreamento e monitoramento dos hábitos dos usuários. Conforme definido por França (2015, p. 96), os *cookies* funcionam como uma "carteira de identidade" digital, permitindo a identificação de usuários e a memorização de suas preferências. Essa tecnologia, introduzida em um contexto de publicidade comportamental[158], tem como principal objetivo viabilizar a formação de perfis detalhados de consumidores, integrando-os ao *marketing* segmentado (*Vide Capítulo 1.2.3.1*) e ao chamado "*marketing one to one*"[159](Souza, 2018, p. 33-34).

Nesse sentido, Raissa Arantes Tobbin e Valéria Silva Galdino Cardin (2021), apontam a existência de uma diversidade de *cookies*, que possuem funcionalidades e finalidades distintas:

---

[158] A publicidade comportamental é uma derivação específica da publicidade interativa, caracterizando-se pela utilização de dados coletados sobre os hábitos e comportamentos online dos usuários para criar anúncios altamente personalizados. Enquanto a publicidade interativa, em seu sentido mais amplo, abrange diversos métodos destinados a tornar os anúncios mais relevantes para os consumidores, como a publicidade contextual e a segmentada, a publicidade comportamental se diferencia por sua capacidade de construir perfis detalhados dos usuários. Essa abordagem permite identificar preferências e padrões de navegação, como páginas visitadas, tempo de permanência e interações realizadas, possibilitando não apenas a personalização de anúncios, mas também o direcionamento preciso de campanhas publicitárias (Souza, 2018, p. 33). Essa derivação reflete o avanço técnico e estratégico no uso de dados, ampliando a eficácia do *marketing*, mas também levantando questões sobre privacidade e ética no tratamento de informações pessoais.

[159] Esse conceito foi desenvolvido pelos americanos Pepper e Roger, que propagaram a necessidade de utilização de bancos de dados de consumidores e de meios interativos para oferecer ao consumidor o máximo de produtos e serviços possíveis, em substituição à antiga máxima de oferecer o mesmo produto à maior quantidade de clientes possíveis (SCHWENKE, Matthias. *Apud*: MENDES, Laura Schertel. 2008

> Os *cookie*s são arquivos que são depositados no computador do indivíduo pelo site acessado e que possibilitam a identificação deste usuário com o intuito de facilitar a funcionalidade da página e o monitoramento da navegação, de forma que podem ser oriundos das páginas visitadas, de outras entidades (*cookies* de terceiros), apagáveis (*cookies* de sessão) ou persistentes (*cookies* permanentes) (CASTELLUCCIA, 2012, p. 23-24). Os principais tipos de cookies seriam (i) os do próprio domínio (primários ou *first party cookies*); (ii) os definidos por terceiros (denominados *third party cookies*), os que somente funcionam enquanto estiver aberta determinada página (*cookie*s de sessão ou *session cookies*) e os que atuam mesmo depois que o site ou página for fechada (*cookies* permanentes) (ALDEIAS, 2012 *apud* FRANÇA, 2015, p. 98) (2021, p. 243-244)

Embora, em teoria, o gerenciamento e o bloqueio de cookies sejam possíveis, a classificação dos "*cookies* permanentes" revela um panorama em que os mecanismos tradicionais de controle se mostram insuficientes para garantir o efetivo gerenciamento dos dados pelo próprio titular (Tobbin; Cardin, 2021, p. 244). Exemplos notáveis dessa categoria incluem os *supercookies* e os *evercookies*. Os *supercookies* utilizam elementos do navegador para gerenciar os dados do usuário, contornando os controles disponíveis e dificultando a exclusão ou limitação da coleta de informações. Por sua vez, os *evercookies* são capazes de manipular o armazenamento temporário de dados (cachê), permanecendo ativos no dispositivo do usuário mesmo após uma aparente exclusão (*Ibidem*).

Ainda que a utilização de *cookies* não seja, em si, ilegal, sua aplicação desregulada e excessiva tem gerado preocupações significativas em termos de privacidade e segurança digital (Souza, 2018, p. 34). Mais, tendo em vista a complexidade do fluxo informacional e as limitações do cidadão comum para um genuíno processo de tomada de decisão (*Vide Capítulo 2.3.1*), fica explícita a necessidade de uma proteção especial que vise a nivelar essa relação.

Tendo como finalidade a personalização de publicidades e conteúdos, os *cookies* corroboram com a criação de "câmaras de eco digitais" (*Vide Capítulo 2.1.2.3*), ao promover um ambiente que prioriza informações consideradas de interesse do usuário. Magrani (2019) observa que, nesse processo, frequentemente são ocultados conteúdos que poderiam ser realmente desejados ou necessários. Essa dinâmica, conhecida como *filter bubble*, pode gerar restrições a direitos fundamentais, como o acesso à informação, a liberdade de expressão e a autonomia individual, além de prejudicar o debate público e a formação de consensos na esfera conectada.

Como observa Doneda (2020), o tratamento automatizado de dados intensifica riscos de exposição, discriminação e vigilância digital, transformando a privacidade em mercadoria. A LGPD tenta abordar essas assimetrias por meio do consentimento informado e medidas de

proteção, mas a superficialidade da percepção de riscos pelos usuários e a evolução contínua das estratégias de monitoramento demandam avanços regulatórios urgentes para garantir transparência e segurança no uso de *cookies* (Tobbin; Cardin, 2021).

3.1.2 A tecnologia que invade, a tecnologia que protege

A relação entre tecnologia e privacidade revela um paradoxo: enquanto as inovações tecnológicas podem comprometer a integridade e os direitos fundamentais dos indivíduos, elas também oferecem ferramentas para a proteção da privacidade informacional, tal como propõem as denominadas Privacy *Enhancing Technologies*[160] (PETs) (Bioni, 2021).

Definidas como tecnologias que reforçam-promovem a privacidade, as PETs exemplificam esse papel dual da tecnologia[161]. Elas se inserem no contexto da metodologia *privacy by design*, que busca integrar medidas de proteção de dados pessoais desde a concepção de sistemas tecnológicos, implementando princípios como confidencialidade, anonimização[162] e prevenção de riscos diretamente em suas arquiteturas (Bioni; Zanatta, 2020).

Para Laura Schertel Mendes e Gabriel da Fonseca (2020), as novas tecnologias não se limitam a gerar benefícios ou malefícios; elas podem produzir ambos os efeitos, dependendo de como são projetadas e utilizadas. Nesse contexto, as PETs desempenham um papel essencial ao combinar inovação tecnológica com autodeterminação informativa, promovendo maior controle dos indivíduos sobre seus dados pessoais. Essas tecnologias auxiliam na complexa tarefa de "regenerar a atrofiada estratégia regulatória", marcada pelo uso extensivo do "consentimento do titular da proteção de dados pessoais" (Bioni, 2021, p. 172). Um exemplo concreto é a "criptografia de ponta a ponta", empregada por aplicativos como o *WhatsApp*, que

---

[160] Esse termo pode ser compreendido como um conceito abrangente, capaz de englobar um conjunto diversificado de tecnologias projetadas para promover, facilitar e assegurar a privacidade, atuando como instrumentos que incorporam diretrizes de proteção de dados diretamente em sua concepção e funcionalidade.

[161] Outras arquiteturas de rede que desempenham um papel relevante como mecanismos para equilibrar ou aprimorar a capacidade dos cidadãos de gerenciar o controle sobre seus dados incluem as *Privacy Invasive Technologies* (PITs), o *Platform for Privacy Preferences Project* (P3P) e o *Do Not Track* (DNT). Para uma análise detalhada, consultar: BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

[162] A anonimização, no âmbito da proteção de dados pessoais, é o processo pelo qual se elimina ou reduz significativamente os elementos identificadores que vinculam dados a seus titulares, tornando-os incapazes de revelar a identidade de uma pessoa. Esse processo pode ser realizado por meio de técnicas como supressão, generalização, randomização e pseudonimização, embora não esteja livre de falhas. Estudos apontam que bases de dados anonimizadas podem ser cruzadas com outras fontes, resultando na reidentificação de indivíduos — um problema agravado pela atuação de *data brokers* (*Vide Capítulo 1.2.2.1*). Esse risco, conhecido como "efeito mosaico", evidencia que dados anonimizados podem, em determinadas circunstâncias, ser revertidos ao *status* de dados pessoais, colocando em questão a efetividade plena da anonimização no contexto da privacidade e proteção de dados (Bioni, 2021).

converte mensagens de texto, voz e vídeo em dados cifrados, permitindo que apenas os participantes da comunicação possam decifrá-los, dificultando interceptações e acessos não autorizados (Abreu, 2017).

A funcionalidade das PETs vai além da proteção passiva. Tecnologias como o *Google Dashboard* permitem que os usuários configurem preferências de privacidade de forma personalizada, oferecendo maior transparência e controle sobre seus dados pessoais (Mendes; Da Fonseca, 2020). Assim, essas ferramentas respondem às limitações das tradicionais políticas de consentimento, que muitas vezes falham em proporcionar efetiva autonomia ao titular dos dados (Lima, 2023).

Ainda que em estágio inicial de desenvolvimento, as PETs apresentam um caminho promissor para a integração da proteção de dados ao próprio funcionamento dos sistemas tecnológicos. Sob essa perspectiva, a tecnologia assume um papel emancipador, promovendo o equilíbrio entre as demandas de um mercado informacional assimétrico e os direitos dos cidadãos em um ambiente digital (Bioni, 2021). Como defende Rubinstein (2011) e Cohen (2000), é essencial que sistemas tecnológicos não apenas atendam às normas jurídicas, mas sejam projetados para incorporar, de forma prática e efetiva, os princípios da segurança e da prevenção previstos na legislação, como na LGPD.

Portanto, a tecnologia tanto pode ser uma ameaça à privacidade quanto uma aliada indispensável na construção de um ambiente digital mais seguro. A integração entre direito e tecnologia, representada pelas PETs, deve continuar sendo explorada e aprimorada, reforçando a confiança dos usuários e garantindo a proteção dos dados pessoais em uma sociedade cada vez mais interconectada.

3.1.3. Repensando o consentimento: desafios e caminhos para uma regulação mais eficaz

O consentimento, fundamento central na regulação da proteção de dados, enfrenta desafios consideráveis para efetivar a autodeterminação informacional em um ambiente digital caracterizado por complexidades técnicas e profundas assimetrias informacionais (*Vide Capítulo 2.3*). Apesar das qualificações previstas na LGPD — como a exigência de ser livre, informado e específico —, sua aplicação prática encontra barreiras estruturais, como a opacidade dos sistemas, a limitação das escolhas dos usuários e a falta de transparência nos fluxos de dados (*Vide Capítulo 1.3.2*). Esses fatores tornam o consentimento insuficiente para garantir, de forma substancial, a proteção dos direitos dos titulares (*Vide Capítulo 2.3.1*).

No atual cenário, o modelo regulatório centrado no consentimento demonstra-se inadequado diante das novas dinâmicas da economia digital, marcadas pela coleta massiva e pelo uso secundário de dados pessoais (*Vide Capítulo 2.2.2*). Reduzido a um formalismo jurídico, o consentimento raramente reflete a autonomia do titular, especialmente em relações permeadas por práticas contratuais compulsórias e desequilíbrios informacionais profundos (*Vide Capítulo 3.1.1*).

Uma hipótese emergente para mitigar essas limitações é a adoção de medidas como a *privacy by design* e as PETs (*Vide Capítulo 3.1.2*). Contudo, para que tais soluções sejam eficazes, é necessária uma readequação da LGPD, incorporando uma abordagem regulatória mais substancial. Essa (re)adequação deve priorizar o controle direto sobre os fluxos informacionais, restringir o uso secundário de dados e fortalecer os mecanismos de fiscalização e responsabilização dos agentes de tratamento (Bioni, 2021).

Essa perspectiva de intervenção parte da ideia de que a proteção de dados precisa ir além do consentimento formal, exigindo uma reorganização normativa que valorize a proteção efetiva da personalidade do indivíduo (Bioni, 2021). Essa reorganização requer um modelo regulatório que trate o consentimento como um elemento complementar dentro de uma estrutura mais abrangente. Tal modelo deve incorporar um discurso de ambivalência, confiando, em certos contextos, na capacidade do indivíduo de gerir seus próprios dados, mas reconhecendo, em outros, a necessidade de intervenção normativa para garantir maior proteção (Bioni, 2021, p. 276).

Nesse sentido, torna-se essencial a criação de uma zona regulatória de interferência alinhada aos princípios da dignidade humana, isonomia e não discriminação, autodeterminação informacional, boa-fé, transparência, minimização de riscos e privacidade contextual. Esses princípios visam a assegurar uma autonomia genuína, coerente com o valor social atribuído à proteção de dados pessoais (*Vide Capítulo 3.3.2).*

Assim, as limitações do consentimento devem ser entendidas não como barreiras, mas como oportunidades para o desenvolvimento de um sistema regulatório mais robusto e adaptado às demandas contemporâneas. Nos próximos capítulos, será discutido como essa transformação pode ser fundamentada em abordagens teóricas sólidas, destacando as contribuições de Stefano Rodotà, Daniel J. Solove e Helen Nissenbaum. Tais reflexões apontam para uma normatização substancial que transcenda o formalismo do consentimento, promovendo uma abordagem intervencionista da LGPD e equilibrando os direitos dos indivíduos com as dinâmicas econômicas e tecnológicas da "sociedade digital".

3.2 FUNDAMENTAÇÕES TEÓRICAS PARA UMA NORMATIZAÇÃO SUBSTANCIAL DE PROTEÇÃO DE DADOS

3.2.1. Stefano Rodotà, e a reorganização do espectro normativo

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso destes dados por parte de tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o indivíduo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em 'controle'. Aliás, a insistência em meios de controle exclusivamente individuais pode ser o álibi de um poder público desejoso de esquivar-se dos novos problemas determinados pelas grandes coletas de informações, e que assim se refugia em uma exaltação ilusória dos poderes do indivíduo, o qual se encontrará, desta forma, encarregado da gestão de um jogo do qual somente poderá sair como perdedor (Rodotà, 2008, p. 37).

O diagnóstico de Stefano Rodotà (2008) é contundente: as normativas tradicionais de proteção de dados, centradas no controle individual, fracassam ao lidar com a assimetria de poder criada pelas tecnologias informacionais (2008). Nesse cenário, o modelo regulatório atual, ancorado na tríade "pessoa-informação-sigilo", revela-se inadequado (2008). A abordagem, ao tratar a privacidade como um simples mecanismo de defesa contra invasões externas, desconsidera a circulação de dados como um elemento central e inevitável das relações econômicas e políticas da "sociedade informacional". Essa concepção estática e individualista não reflete as dinâmicas contemporâneas, marcadas pela integração de dados pessoais em sistemas globais e pelo uso dessas informações como mercadorias estratégicas (2008).

Rodotà argumenta que essa abordagem limitada perpetua uma ilusão de controle e autonomia, ao mesmo tempo que exime o poder público de sua responsabilidade de regulamentar a circulação de dados de forma efetiva (2008). O indivíduo, isolado, é incapaz de enfrentar o poder de organizações que possuem recursos avançados para coletar e manipular informações, o que o coloca em uma posição de desvantagem estrutural (2008). Nesse contexto, a insistência no consentimento individual como principal fundamento normativo para o tratamento de dados é criticada como insuficiente para lidar com a complexidade dos fluxos informacionais atuais (2008).

Para superar essas limitações, Rodotà propõe a reorganização do espectro normativo por meio da tríade "pessoa-informação-circulação" (2008). Diferentemente do paradigma baseado no sigilo[163], sua abordagem reconhece a circulação de dados como um fenômeno inevitável e estrutural das sociedades contemporâneas. Assim, a privacidade deixa de ser entendida como um direito meramente defensivo e passa a ser integrada a um modelo regulatório coletivo, que considera os fluxos de informações não apenas como uma ameaça, mas também como uma oportunidade para promover justiça social e equilíbrio de poder (2008).

Central à proposta de Rodotà é o deslocamento do foco regulatório da autodeterminação informacional para o controle social. Ele defende a criação de mecanismos que integrem transparência, *accountability*[164] e ética no tratamento de dados, permitindo que as relações entre indivíduos e grandes organizações informacionais sejam reequilibradas (2008). A regulamentação, nesse modelo, não busca apenas proteger o indivíduo, mas também estabelecer sistemas que promovam redistribuição equitativa do poder informacional, combatendo abusos estruturais e garantindo que a circulação de dados seja compatível com os direitos fundamentais e a dignidade humana (2008).

A transição para esse novo paradigma exige também a revisão do papel do consentimento individual. Para Rodotà (2008), o consentimento deve ser complementado por princípios normativos que regulem o fluxo de informações com base em critérios coletivos e globais, reconhecendo a interdependência entre os interesses individuais e os benefícios sociais mais amplos. Isso inclui a implementação de uma infraestrutura normativa que não apenas proteja os dados, mas também regule sua circulação de forma a promover a equidade e a inclusão social.

Com essa reorganização normativa, Rodotà (2008) redefine o papel da privacidade no contexto da "sociedade informacional". Ao substituir a tríade "pessoa-informação-sigilo" por "pessoa-informação-circulação", Stefano Rodotà (2008) aponta para a necessidade de um

[163] Embora o modelo normativo proposto por Stefano Rodotà priorize a circulação e o controle das informações, o autor (2008) enfatiza que o sigilo e a proteção dos dados pessoais permanecem pilares essenciais do direito à privacidade, não podendo ser negligenciados. Ele aponta que a necessidade de proteção informacional se expandiu além da esfera estritamente íntima, abrangendo dados cuja circulação pode gerar discriminação ou prejuízos aos titulares, como informações relacionadas à saúde, hábitos sexuais, opiniões políticas e sindicais, bem como aspectos étnico-raciais e crenças religiosas. Apesar de muitas dessas informações estarem inseridas na esfera pública, Rodotà defende uma abordagem normativa que assegure sua proteção, incluindo a proibição de coleta por determinados sujeitos, como empregadores, para prevenir usos abusivos ou discriminatórios. Isso demonstra que o sigilo continua a desempenhar um papel estrutural e indispensável na regulação da privacidade, mesmo em um contexto no qual a circulação de dados assume centralidade.

[164] Embora Rodotà não mencione explicitamente o termo *accountability*, suas propostas e conceitos estão em plena consonância com esse princípio. Esse alinhamento pode ser observado, em especial, no capítulo 10, intitulado "por uma estratégia jurídica integrada", de sua obra: a vida na sociedade da vigilância: a privacidade hoje (2008).

modelo que integre a proteção individual e os desafios coletivos impostos pela economia digital. Esse paradigma não apenas responde às insuficiências do modelo tradicional, mas também inaugura um horizonte normativo mais abrangente e robusto, no qual a privacidade e a circulação de dados coexistem como pilares fundamentais de uma sociedade mais justa e equilibrada.

3.2.2. O diagnóstico de Daniel James Solove e algumas reflexões indispensáveis

Daniel J. Solove (2013; 2014) apresenta uma crítica sistemática ao modelo regulatório tradicional de autogestão informacional, propondo uma reestruturação que reconheça as limitações práticas do consentimento e incorpore soluções que considerem os desafios cognitivos e estruturais impostos pela economia digital. Sua análise está fundamentada na percepção de que o consentimento, embora um elemento importante, não é suficiente para assegurar uma proteção efetiva dos direitos de privacidade no cenário atual (2013).

Solove identifica dois eixos problemáticos no modelo vigente: os problemas cognitivos e os estruturais. No aspecto cognitivo, ele argumenta que a estrutura de autogestão da privacidade pressupõe que os indivíduos são informados, racionais e capazes de tomar decisões conscientes e fundamentadas sobre o tratamento de seus dados (2013). Contudo, pesquisas[165] indicam que a maioria das pessoas não lê ou compreende os termos de uso e políticas de privacidade, sendo incapaz de avaliar adequadamente os riscos associados à coleta e ao uso de suas informações (2013). Essa sobrecarga decisória, combinada com a assimetria de informações, transforma o consentimento em um ato simbólico e muitas vezes desconectado da realidade prática (2013).

No campo estrutural, Solove (2013) destaca que a fragmentação da coleta e o tratamento cumulativo de dados por múltiplas entidades tornam impossível para os indivíduos o exercício de controle efetivo sobre suas informações. A agregação de dados ao longo do tempo, somada à opacidade tecnológica, dificulta a identificação de riscos e a compreensão dos impactos a

[165] Conforme aponta o estudo de Florencia Marotta-Wurgler (2011), mesmo com o aumento da acessibilidade e exigências como os *clickwraps* – que demandam que o usuário clique em "eu concordo" –, a taxa de leitura de termos de uso ou políticas de privacidade permanece surpreendentemente baixa. A pesquisa revela que apenas entre 0,1% e 1% dos usuários realmente leem esses contratos, mesmo em cenários nos quais o acesso é facilitado. A diferença entre os *clickwraps* e os *browsewraps* – termos que não requerem aceitação explícita – é insignificante, com os *clickwraps* sendo lidos apenas 0,36% mais frequentemente, em média, conforme seis estimativas analisadas. Esses dados ainda são conservadores, pois incluem como leitores todos os usuários que acessaram a página do contrato por pelo menos um segundo, embora um contrato típico de licença contenha aproximadamente 2.300 palavras e seja escrito em linguagem jurídica complexa.

longo prazo. Isso é agravado pelo fenômeno do uso secundário de dados, em que as informações coletadas originalmente para uma finalidade são reutilizadas para propósitos distintos, muitas vezes desconhecidos pelos titulares.

Diante das limitações do consentimento[166] como principal elemento da autogestão da privacidade, Solove (2013) sugere uma abordagem regulatória que transcenda sua dependência exclusiva, focando na proteção substantiva da privacidade. O autor critica a legislação vigente[167] por oferecer pouca orientação sobre formas adequadas de coleta, uso e divulgação de dados e destaca a necessidade de estabelecer limites claros, ainda que sem adotar um modelo estritamente paternalista[168] (2013).

A proposta de Daniel Solove destaca a necessidade de padrões de minimização de dados, restringindo a coleta apenas ao que for estritamente necessário e à proibição de determinados usos, mesmo que consentidos, quando apresentarem riscos significativos aos direitos fundamentais (2013). Além disso, o autor defende a criação de mecanismos regulatórios que promovam uma transparência real, permitindo que os indivíduos tenham acesso claro às informações sobre o uso de seus dados. Solove (2014) também sugere o fortalecimento da responsabilização dos controladores de dados, por meio de auditorias regulares, avaliações de impacto e a adoção de práticas preventivas – *e.g., privacy by design* – para evitar riscos à privacidade antes que estes se concretizem.

Ademais, Solove (2013) argumenta que a privacidade deve ser reconhecida como um bem coletivo, cujos impactos transcendem os indivíduos diretamente afetados, influenciando temas sociais amplos como inovação, democracia e dignidade humana. Sua crítica inclui o

---

[166] Daniel Solove (2013) argumenta que, apesar das falhas da autogestão da privacidade, o consentimento continua sendo um elemento essencial. Ele defende que oferecer aviso, acesso e controle sobre os dados pessoais é fundamental para garantir autonomia em um contexto de crescente uso de dados, decisões automatizadas e justificativas opacas, permitindo que as pessoas compreendam e influenciem como seus dados são utilizados.

[167] Daniel Solove, ao criticar a legislação vigente, refere-se ao papel desempenhado pela *Federal Trade Commission* (FTC) como reguladora primária da privacidade nos Estados Unidos. A FTC, criada em 1914, é uma agência independente do governo norte-americano responsável por proteger os consumidores e promover a concorrência. No contexto da privacidade, a FTC utiliza sua autoridade para combater práticas comerciais injustas e enganosas, fiscalizando as políticas de privacidade das empresas. No entanto, Solove (2014) aponta que, apesar de seu impacto significativo, a atuação da FTC possui lacunas, como a dependência de acordos extrajudiciais em vez de decisões judiciais e a falta de padrões robustos para limitar a coleta e o uso de dados, deixando grandes áreas da economia digital sem regulamentação clara.

[168] No entendimento do autor, evitar uma abordagem paternalista na regulação da privacidade significa não impor proibições absolutas e inflexíveis à coleta e uso de dados, mas sim buscar um equilíbrio entre proteção e autonomia individual. Solove (2013) argumenta que a legislação deve adotar uma postura proativa, estabelecendo limites claros para práticas que coloquem em risco direitos fundamentais, mas sem eliminar a possibilidade de os indivíduos exercerem algum controle sobre suas informações. Daniel (2014) ressalta que essa abordagem deve priorizar padrões que protejam contra usos abusivos e riscos significativos, ao mesmo tempo em que reconhece a importância do consentimento como um elemento complementar de autonomia informacional.

alerta de que um modelo centrado excessivamente no consentimento frequentemente legitima práticas invasivas ao invés de preveni-las, exigindo uma abordagem mais intervencionista, capaz de equilibrar autonomia individual e proteção dos direitos fundamentais em um contexto digital cada vez mais complexo e assimétrico.

3.2.3 A disruptiva "privacidade contextual" de Helen Nissenbaum

A obra "*Privacy in context*", de Helen Nissenbaum (2010), apresenta uma reformulação teórica inovadora da privacidade, abordando-a como um fenômeno essencialmente contextual (2010). Diferentemente das abordagens tradicionais, que restringem a privacidade ao controle individual de dados pessoais, Nissenbaum propõe o conceito de privacidade contextual, fundamentado nas normas sociais específicas de cada contexto (2010). Essas normas, denominadas normas informacionais, regulam as condições de acesso, uso e transmissão de informações pessoais, refletindo expectativas, valores e objetivos sociais próprios de diferentes esferas da vida cotidiana, como saúde, educação, trabalho e lazer[169] (2010). A privacidade, nessa perspectiva, está vinculada à conformidade dos fluxos informacionais com essas normas e sua violação ocorre quando práticas informacionais desrespeitam as "legítimas expectativas"[170] compartilhadas, comprometendo tanto os direitos individuais quanto a estabilidade social (2010).

Para Nissenbaum, a privacidade não é uma entidade universal ou fixa, mas um fenômeno relacional, moldado pelas dinâmicas culturais, históricas e tecnológicas de cada contexto (2010). A autora destaca que o avanço das TICs introduziu práticas disruptivas de coleta, armazenamento e uso de dados, muitas vezes incompatíveis com as normas sociais preexistentes (2010). Esse descompasso gera ansiedade, resistência e desconfiança, comprometendo a legitimidade dos sistemas informacionais (2010). O conceito de privacidade contextual oferece uma estrutura analítica para compreender e normatizar essas práticas, priorizando a adequação dos fluxos informacionais às regras específicas que sustentam o funcionamento dos diversos contextos sociais (2010). Por exemplo, enquanto o

[169] Conforme Bioni (2021), a privacidade contextual concentra-se em compreender a dinâmica do tráfego informacional a partir da relação que o origina – considerada a causa principal para a coleta e o tratamento de dados pessoais – e, em seguida, analisar como terceiros podem intervir nesse processo. Nesse contexto, a pesquisa prioriza investigar como a dinâmica do fluxo de dados pessoais no mercado informacional, que inclui rastreamento e compartilhamento com terceiros, pode ser impactada por esse novo enquadramento normativo.

[170] A expressão "legítima expectativa" traz consigo dois elementos adensados na cultura jurídico-nacional: o princípio da "boa-fé" e da "confiança", sendo o primeiro expressamente previsto na LGPD (art. 6°, *caput*).

compartilhamento de informações médicas entre profissionais de saúde para diagnóstico é legítimo, a utilização dessas mesmas informações para fins de *marketing* constitui uma grave violação das normas informacionais do setor[171] (2010).

A privacidade contextual também representa uma crítica às abordagens universalistas, que buscam impor padrões homogêneos de privacidade a todos os contextos (2010). Nissenbaum argumenta que essas teorias são insuficientes, pois ignoram as especificidades culturais e sociais que moldam as expectativas normativas de diferentes esferas (2010). Em vez disso, ela defende uma abordagem flexível e adaptativa, que reconheça a historicidade e a mutabilidade das normas informacionais, permitindo que estas evoluam em resposta às transformações culturais e tecnológicas (2010). Nesse sentido, a privacidade contextual proporciona um modelo mais robusto e aplicável, capaz de lidar com a complexidade das interações mediadas por tecnologia, ajustando-se às particularidades de cada ambiente (2010).

A aplicabilidade do conceito de privacidade contextual é ampla e relevante, especialmente para a formulação de políticas públicas e regulamentações de proteção de dados (2010). Em vez de se limitar ao consentimento individual[172] ou à anonimização de dados, como fazem as abordagens tradicionais, a privacidade contextual exige que as práticas informacionais sejam avaliadas com base na conformidade às normas sociais do contexto em que ocorrem (2010). Isso inclui não apenas a análise de quem tem acesso às informações e como elas são utilizadas, mas também o alinhamento dessas práticas aos valores e objetivos coletivos do ambiente (2010). No campo tecnológico, Nissenbaum (2010) sugere que os sistemas sejam projetados para respeitar as normas informacionais específicas, incorporando mecanismos que assegurem maior transparência e responsabilização[173]. Já no âmbito jurídico, a privacidade contextual oferece critérios claros para avaliar conflitos envolvendo o uso de dados, como na

---

[171] Para Bioni (2021), a aplicação do instituto do abuso de direito, amplamente consagrado na cultura jurídica brasileira, representa um importante contrapeso à legítima expectativa no contexto do tráfego de informações pessoais. Nesse cenário, a cláusula geral do CC ganha relevância ao delimitar os atos ilícitos relacionados ao uso de informações pessoais, especialmente quando excedem os limites impostos pelo fim econômico ou social, pela boa-fé e pelos bons costumes. O abuso de direito, portanto, atua como uma via de ingresso para a imposição de limites éticos e sociais às atividades envolvendo TICs e comunicação, refletindo a crescente relevância da ética nos debates regulatórios. Assim, mais do que reconhecer o abuso de direito como ferramenta para balizar a privacidade contextual no Brasil, é essencial analisar como a LGPD contribui teleologicamente para fortalecer essa delimitação jurídica.

[172] Segundo Bioni (2021), avaliar se o fluxo informacional é adequado ou inadequado requer a limitação do uso do consentimento, considerando o impacto que a circulação de informações pessoais exerce sobre as relações sociais do titular, especialmente no que diz respeito ao livre desenvolvimento de sua personalidade. Assim, o consentimento do titular não pode servir como instrumento para legitimar práticas abusivas e invasivas de tratamento de dados pessoais, que reduzem o indivíduo a uma condição de mero objeto.

[173] *E.g., privacy by design* e *privacy by default.*

vigilância governamental, no monitoramento de trabalhadores e na publicidade dirigida por algoritmos. Nessas situações, a legitimidade das práticas informacionais deve ser avaliada pela conformidade com as expectativas contextuais, em vez de critérios abstratos ou generalistas.

Além disso, a privacidade contextual fornece uma base teórica sólida para normatizações substanciais na proteção de dados. Políticas públicas orientadas por essa abordagem podem exigir que as organizações identifiquem e respeitem as normas informacionais de cada contexto como condição para o uso legítimo de informações pessoais. Isso inclui a realização de avaliações de impacto de privacidade que considerem aspectos sociais e culturais, além de fatores técnicos. Também implica no desenvolvimento de mecanismos de governança adaptáveis, capazes de responder às rápidas transformações tecnológicas que reconfiguram os contextos informacionais. Ao situar a privacidade no cerne das interações sociais, a abordagem contextual transcende as limitações das concepções universalistas, oferecendo uma estrutura normativa adaptativa que reflete as complexidades da sociedade contemporânea (Nissenbaum, 2010).

Dessa forma, a privacidade como integridade contextual[174], redefine a privacidade como um fenômeno normativo e relacional, profundamente conectado às normas que regulam os fluxos de informações nos diferentes contextos sociais). Ao transcender a visão reducionista de controle individual, a privacidade contextual proporciona um modelo teórico dinâmico e pragmático que oferece diretrizes aplicáveis para enfrentar os desafios éticos, jurídicos e tecnológicos da era digital. Essa abordagem se fundamenta na premissa de que a proteção de dados não pode ser eficaz sem uma atenção rigorosa às especificidades dos contextos em que os fluxos informacionais ocorrem, constituindo, assim, uma base indispensável para uma normatização substancial da proteção de dados (Nissenbaum, 2010).

3.3 REPENSANDO O PARADIGMA NORMATIVO: UMA ABORDAGEM CONCLUSIVA PARA A LEI 13.709/2018

A análise desenvolvida no capítulo 3.2 revela um ponto de convergência significativo entre os diagnósticos de Stefano Rodotà, Daniel J. Solove e Helen Nissenbaum: a inadequação do modelo normativo centrado preponderantemente no consentimento individual para enfrentar

[174] A integridade contextual, segundo Helen Nissenbaum (2004), refere-se à conformidade dos fluxos de informação com as normas informacionais de um contexto específico, que determinam quem pode acessar, usar ou transmitir dados pessoais e sob quais condições. A privacidade, nessa perspectiva, é preservada quando esses fluxos respeitam as expectativas normativas do contexto social em questão.

as complexidades da sociedade informacional e da economia digital. Apesar de cada autor abordar o tema da privacidade sob diferentes perspectivas, suas reflexões apontam para a necessidade de repensar a estrutura regulatória em prol de alternativas mais robustas, capazes de lidar com as assimetrias de poder, a opacidade dos fluxos informacionais e a fragmentação das relações entre titulares e controladores de dados.

Rodotà (2008) enfatiza que a insistência em um controle exclusivamente individual sobre os dados pessoais perpetua uma ilusão de autonomia, desconsiderando o desequilíbrio estrutural entre os indivíduos e as organizações que controlam e processam informações em escala global. A proposta de deslocar o foco regulatório para o controle social e a redistribuição de poder informacional fornece uma base normativa mais equitativa e ajustada às dinâmicas contemporâneas.

Solove (2013; 2014), ao identificar as limitações práticas do consentimento, evidencia que o modelo tradicional falha em abordar problemas estruturais, como o uso secundário de dados e a opacidade das práticas de coleta e processamento. Ele argumenta haver necessidade de uma regulação que vá além do consentimento e incorpore padrões de minimização de dados[175], responsabilização proativa e restrições a usos abusivos, mesmo que consentidos.

Nissenbaum (2010), por sua vez, desloca a análise para a dimensão contextual, sugerindo que a privacidade deve ser avaliada com base na conformidade das práticas informacionais às normas sociais específicas de cada contexto. Essa abordagem reconhece que o consentimento, em sua forma tradicional, não captura a complexidade das expectativas normativas que variam entre diferentes esferas da vida social e da interação mediada por tecnologia.

A partir dessas convergências, é possível diagnosticar que o modelo regulatório da LGPD, centrado na autodeterminação informacional por meio do consentimento, precisa ser ampliado para incluir mecanismos mais substantivos e coletivos. Embora a LGPD traga avanços importantes, como os princípios de *accountability* e *privacy by design*[176], ela ainda

[175] A LGPD adota o princípio da minimização de dados, estabelecido no artigo 6º, inciso III, como um dos pilares para o tratamento de dados pessoais. Esse princípio determina que o tratamento deve se limitar ao mínimo necessário para a realização de suas finalidades, ou seja, os dados coletados devem ser estritamente adequados, pertinentes e proporcionais ao propósito específico para o qual são utilizados. Contudo, a LGPD tem enfrentadoproblemas para consolidar efetivamente a aplicação desse princípio (*Vide Capítulo 3.3.1*).

[176] A LGPD incorpora os princípios de *accountability* e *privacy by design* em diferentes disposições. O princípio da *accountability* encontra respaldo no art. 6º, X, ao exigir que os agentes de tratamento de dados demonstrem a adoção de medidas eficazes e capazes de comprovar a conformidade com as normas de proteção de dados pessoais. Já o conceito de *privacy by design*, embora não expressamente mencionado, está implícito no art. 46, que estabelece a obrigatoriedade de implementação de medidas técnicas e administrativas voltadas à segurança dos

carece de instrumentos que ajudem a enfrentar diretamente os desafios estruturais e culturais impostos pela "sociedade da informação". Assim, alternativas normativas mais robustas podem ser construídas a partir das seguintes premissas:

1. Reconhecimento das limitações do consentimento: a legislação deve superar o paradigma do consentimento como principal fundamento para o tratamento de dados, incorporando medidas que abordem as vulnerabilidades estruturais e informacionais dos titulares.

2. Fortalecimento da responsabilidade dos agentes de tratamento: implementar mecanismos de fiscalização, auditorias e avaliações de impacto que ampliem a *accountability* e promovam uma transparência real nas práticas informacionais.

3. Integração de princípios contextuais: adotar abordagens que respeitem as normas sociais específicas de cada contexto, permitindo que as práticas informacionais sejam avaliadas de forma dinâmica e adaptativa.

A LGPD, nesse sentido, encontra-se diante de uma oportunidade de evolução normativa que precisa ir além do formalismo do consentimento, explorando caminhos que combinem governança ética, tecnologias protetivas e uma visão mais inclusiva da privacidade como bem social. A convergência das críticas teóricas reforça a urgência de um modelo regulatório mais amplo e eficaz, alinhado às demandas da sociedade contemporânea.

3.3.1 O uso secundário dos dados pessoais: desafios e limites

O uso secundário de dados pessoais é definido por Daniel Solove (2006, p. 519) como "o uso de dados para propósitos não relacionados aos propósitos para os quais os dados foram inicialmente coletados sem o consentimento do titular dos dados". Esse fenômeno decorre do crescimento exponencial da *big data* e das tecnologias que permitem o armazenamento e processamento massivo de informações (*Vide Capítulo 2.2.2.1*). Embora promova inovações e benefícios econômicos, essa prática levanta preocupações éticas e jurídicas, especialmente no que tange à privacidade e à transparência no tratamento de dados (Solove, 2006).

Nesse contexto, a LGPD introduz mecanismos e princípios para reduzir os riscos associados ao uso secundário de dados pessoais, buscando compatibilizar a evolução tecnológica com a salvaguarda dos direitos fundamentais dos titulares. O princípio da

dados, e no art. 50, §2º, II, que preconiza a necessidade de incorporar mecanismos de proteção à privacidade desde a concepção de produtos, serviços e processos.

finalidade, consagrado no art. 6º, I, da LGPD, exige que os dados sejam tratados exclusivamente para os fins específicos, legítimos, explícitos e informados no momento da coleta, impedindo sua reutilização para propósitos incompatíveis ou não previstos inicialmente. Qualquer alteração ou ampliação da finalidade demanda justificativa detalhada pelo controlador, que deve assegurar a conformidade com os critérios de necessidade, adequação e proporcionalidade previstos na legislação[177] (DOZZA, 2023, p. 44). Essa disposição normativa tem como objetivo mitigar práticas abusivas e proteger a autodeterminação informativa dos titulares, evitando que seus dados sejam manipulados de forma arbitrária ou imprevisível.

O princípio do legítimo interesse, previsto nos arts. 7º, IX, e 10 da LGPD, configura uma base legal que oferece maior flexibilidade aos controladores de dados ao permitir o tratamento de informações pessoais para atender a interesses legítimos de operadores e controladores (Bioni, 2021). No entanto, trata-se de um conceito jurídico indeterminado, cujo conteúdo e limites não são previamente definidos, demandando uma avaliação cuidadosa de sua conformidade (Dozza, 2023). Essa flexibilidade apresenta riscos, como a expansão indevida das finalidades originais, potencialmente comprometendo direitos fundamentais e gerando incertezas regulatórias, especialmente no contexto do uso secundário de dados (Solove, 2006). Para assegurar a compatibilidade dessa base legal com os princípios da proteção de dados, sua aplicação – no contexto pós LGPD – exige um teste rigoroso[178], inspirado no modelo do Grupo de Trabalho 29 da União Europeia[179], que analisa proporcionalidade, previsibilidade e impacto

[177] Segundo Bruno Ricardo Bioni (2021), o princípio da limitação de propósitos está fundamentado na estreita relação entre a especificação de uma finalidade e o consentimento. Esse princípio determina que os dados pessoais sejam utilizados exclusivamente para o objetivo previamente autorizado, de forma que qualquer desvio ou ampliação de sua aplicação exija a obtenção de um novo consentimento, assegurando, assim, a proteção dos direitos do titular e a transparência no tratamento das informações.

[178] O princípio do legítimo interesse na LGPD é submetido a um teste rigoroso, inspirado no modelo europeu, para equilibrar os direitos do titular dos dados e os interesses do controlador. Esse teste, frequentemente denominado "*Legitimate Interests Assessment*" (LIA), é dividido em quatro etapas: as três primeiras são conduzidas pelo controlador para avaliar a legitimidade do interesse, sua necessidade e a proporcionalidade do tratamento, enquanto a quarta etapa oferece espaço para o contraditório e a ampla defesa do titular ou de entidades que o representem. Esse modelo, detalhado no art. 10 da LGPD, busca assegurar a aplicação criteriosa dessa base legal, evitando abusos e alinhando-se aos princípios da boa-fé, da legítima expectativa e da proteção aos direitos fundamentais, em especial à autodeterminação informacional (Bioni, 2021).

[179] O Grupo de Trabalho do Artigo 29, vinculado à União Europeia, formulou diretrizes específicas sobre a aplicação da base legal do legítimo interesse, com o objetivo de trazer previsibilidade e segurança jurídica para sua utilização em todo o bloco econômico, além de evitar que essa base fosse utilizada como um artifício para contornar os direitos e princípios estabelecidos pela legislação de proteção de dados. Dentre suas contribuições, destaca-se a elaboração de um teste multifatorial, que orienta tanto reguladores quanto controladores na avaliação da proporcionalidade e adequação do uso dessa base legal, garantindo um equilíbrio entre inovação e proteção de direitos fundamentais (Bioni, 2021). Veja, nesse sentido: *ARTICLE 29, Data protection working party. Opinion on 06/24 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. Disponível em: <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>.

sob a perspectiva do titular, alinhando-se aos critérios de necessidade e adequação do tratamento pretendido (Bioni, 2021).

O grande problema que o uso secundário pode causar é a utilização dos dados coletados de maneira que o titular dos dados não entenda, no mínimo, desejável (Solove, 2006). Ele frustra as expectativas legítimas do usuário, indo, muitas vezes, contra a boa-fé esperada. O argumento comumente usado pelos "capitalistas de vigilância" é que o titular não possui uma legítima expectativa de proteção quando consente no tratamento de seus dados (Garcia, 2020). Para abordar esse tema, a LGPD incorpora o princípio da transparência – art. 9º – e impõe a obrigação de elaboração de relatórios de impacto à proteção de dados para situações que envolvam maior risco aos direitos dos titulares – art. 38.

No entanto, a LGPD enfrenta desafios significativos na regulamentação do legítimo interesse e na eficácia do relatório de impacto à proteção de dados (RIPD). Apesar de prever a necessidade de justificar o uso do legítimo interesse por meio de critérios como necessidade e proporcionalidade – art. 10 –, a ausência de parâmetros detalhados compromete a previsibilidade e a segurança jurídica na aplicação prática (Dozza, 2023). Além disso, a não obrigatoriedade de elaboração do RIPD em todas as situações de risco elevado, limita sua eficácia como ferramenta preventiva de proteção. Essa lacuna normativa reforça a dependência do titular, que, diante da assimetria informacional e da complexidade técnica, frequentemente não consegue exercer controle efetivo sobre seus dados pessoais (Bioni, 2021). Tal cenário demonstra a necessidade de revisões legislativas que incluam diretrizes mais específicas para o legítimo interesse e para a obrigatoriedade do RIPD, especialmente em contextos de maior sensibilidade.

3.3.2 Regulação do risco: um modelo dinâmico e adaptativo

A regulação do risco emerge como uma abordagem indispensável para complementar o modelo normativo centrado no consentimento, enfrentando as limitações práticas de proteção de dados no ambiente digital contemporâneo. Como observado por Stefano Rodotà (2008), o controle individual sobre dados é insuficiente diante da assimetria de poder entre titulares e grandes organizações, o que exige uma regulação que vá além do consentimento, incorporando estruturas normativas mais amplas. Nesse contexto, práticas como *privacy by design*, "avaliações de impacto" e fiscalização contínua ganham relevância para assegurar um equilíbrio entre inovação tecnológica e proteção de direitos fundamentais.

A *privacy by design*, prevista no art. 46, §2º, da LGPD, reflete a necessidade de integrar a proteção de dados desde a concepção de sistemas tecnológicos. Contudo, em convergência com o diagnóstico de Daniel Solove (2013), a dependência excessiva de consentimentos formais e a ausência de diretrizes claras sobre como implementar princípios como a minimização de dados tornam essa previsão normativa limitada. A LGPD poderia avançar quanto a detalhar critérios específicos que orientassem agentes de tratamento na adoção de soluções tecnológicas preventivas, garantindo maior alinhamento com os objetivos de proteção de dados.

Além disso, o RIPD, previsto no art. 38 da LGPD, poderia desempenhar um papel central na regulação do risco. No entanto, como destaca Helen Nissenbaum (2010), práticas informacionais só são legítimas quando atendem às normas e expectativas contextuais. A ausência de requisitos claros para a elaboração dos RIPDs limita sua eficácia, especialmente ao desconsiderar os aspectos sociais e culturais que envolvem o tratamento de dados. Incorporar a perspectiva de Nissenbaum à LGPD implicaria exigir que esses relatórios considerassem não apenas os riscos técnicos, mas também os impactos éticos e contextuais associados às práticas informacionais.

A fiscalização contínua, essencial para garantir o cumprimento da legislação, também enfrenta desafios práticos. Rodotà (2008) argumenta que a ausência de mecanismos de supervisão eficazes perpetua a vulnerabilidade dos titulares em relação aos controladores de dados. A LGPD reconhece o papel da ANPD na fiscalização, mas a falta de autonomia financeira e infraestrutura técnica da autoridade compromete sua atuação, especialmente no monitoramento de algoritmos e sistemas baseados em *big data*. Um modelo mais robusto de regulação do risco demandaria o fortalecimento da ANPD, com recursos suficientes para auditorias regulares e fiscalização ativa, alinhando-se à proposta de Rodotà de um controle social sobre os fluxos de dados.

Ademais, Solove (2013) observa que a transparência é um dos principais desafios na proteção de dados devido à complexidade dos sistemas digitais e à falta de ferramentas acessíveis para os titulares. Nesse sentido, a LGPD deveria promover o empoderamento dos titulares por meio de mecanismos tecnológicos que lhes permitam controlar ativamente suas informações, como painéis de privacidade personalizáveis. Isso reduziria a assimetria informacional e fortaleceria a autodeterminação informativa, conforme os princípios defendidos por Nissenbaum, ao alinhar os fluxos de dados às expectativas contextuais, e por Solove, ao proporcionar controle mais substancial aos indivíduos.

Dessa forma, a regulação do risco, inspirada nos entendimentos de Rodotà, Nissenbaum e Solove, oferece uma base mais adaptativa e dinâmica para enfrentar as limitações da LGPD. Ao reforçar medidas como *privacy by design*, a reestruturação dos RIPDs, o fortalecimento da ANPD e o desenvolvimento de tecnologias voltadas para o empoderamento dos titulares, a legislação pode evoluir para um modelo que concilie inovação tecnológica com a proteção efetiva dos direitos fundamentais.

CONSIDERAÇÕES FINAIS

A presente pesquisa teve como objeto o alcance material do consentimento do titular, nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD), analisando sua funcionalidade e eficácia no contexto das dinâmicas digitais contemporâneas. Inserido em um cenário dominado pelo capitalismo de vigilância e por práticas informacionais frequentemente opacas, o estudo revelou que o consentimento, enquanto mecanismo normativo central encontra severas limitações conceituais e práticas, tornando-se, muitas vezes, um instrumento insuficiente para mitigar as assimetrias de poder e promover a autodeterminação informacional.

O trabalho demonstrou que a configuração atual do consentimento, baseada em extensos termos de uso e linguagem técnica, falha ao promover uma escolha genuinamente informada por parte do titular de dados. A análise revelou que, em muitos casos, o consentimento é um ato meramente formal, incapaz de proporcionar uma real proteção aos direitos dos indivíduos, principalmente em contextos onde a coleta e o tratamento de dados ocorrem de forma intrusiva e desproporcional. Essa fragilidade é agravada pela assimetria informacional entre titulares e controladores, onde o titular, frequentemente hipervulnerável, é compelido a aceitar condições contratuais que não compreende plenamente.

Ao longo do estudo, foi possível mapear alternativas regulatórias que superem as limitações do modelo centrado no consentimento. Princípios como a privacidade contextual, a minimização de dados e a transparência nos processos de tratamento emergem como ferramentas normativas indispensáveis para reequilibrar as relações entre titulares e controladores. Além disso, a pesquisa trouxe à tona a necessidade de uma abordagem sistêmica e interseccional, considerando como a proteção de dados se relaciona com direitos humanos, inclusão digital e governança ética.

Embora a LGPD represente um marco regulatório de grande relevância no ordenamento jurídico brasileiro, suas lacunas operacionais comprometem sua eficácia. Conceitos como “legítimo interesse” e “finalidade” são, muitas vezes, vagos e dependem de interpretações casuísticas, o que fragiliza a uniformidade e a previsibilidade na aplicação da lei. Essa situação não apenas aumenta a incerteza jurídica, mas também favorece práticas abusivas por parte de controladores, que exploram as ambiguidades normativas para legitimar tratamentos de dados desproporcionais.

Adicionalmente, a ausência de regulamentação específica para tecnologias emergentes, como inteligência artificial, aprendizado de máquina e dispositivos de Internet das Coisas (IoT),

representa um desafio significativo. Essas tecnologias operam com bases de dados massivas e são capazes de gerar impactos profundos sobre os direitos fundamentais dos titulares. Sem um marco normativo claro, essas práticas podem perpetuar discriminações algorítmicas, amplificar desigualdades estruturais e comprometer a dignidade humana.

A pesquisa destacou o papel central da Autoridade Nacional de Proteção de Dados (ANPD) na efetivação da LGPD. No entanto, sua estrutura atual, limitada em recursos e autonomia, impede que desempenhe suas funções de maneira plena. É essencial que a ANPD seja dotada de maior independência, recursos técnicos e humanos, além de mecanismos que garantam sua atuação responsiva e baseada em evidências.

A regulação por riscos, amplamente defendida neste estudo, deve ser incorporada como eixo central das estratégias normativas. Isso inclui a exigência de relatórios de impacto à proteção de dados (RIPD), integrados a auditorias frequentes e metodologias de mensuração de riscos. Tal abordagem permite não apenas mitigar danos potenciais, mas também antecipar problemas decorrentes de práticas informacionais emergentes, promovendo um ambiente regulatório mais dinâmico e adaptativo.

Um ponto central que emerge deste trabalho é a relação intrínseca entre proteção de dados e direitos humanos. O tratamento de dados não pode ser analisado apenas sob a ótica individualista, mas deve ser entendido como uma questão coletiva e sistêmica, que impacta diretamente a igualdade informacional, a justiça social e o fortalecimento da cidadania digital.

Temas como discriminação algorítmica e exclusão digital demandam atenção urgente. A pesquisa revelou que algoritmos, frequentemente tratados como ferramentas neutras, podem perpetuar preconceitos históricos e reforçar desigualdades sociais. Além disso, a exclusão digital, caracterizada pela falta de acesso às tecnologias da informação, agrava a vulnerabilidade de populações marginalizadas, privando-as dos benefícios econômicos e sociais da era digital.

Nesse sentido, é imperativo que futuras pesquisas aprofundem a análise de como a regulação de dados pode ser utilizada como um instrumento de justiça social. Por exemplo, o desenvolvimento de um marco normativo para a inteligência artificial, que inclua auditorias obrigatórias e exigências de transparência algorítmica, pode ser um passo importante para garantir que essas tecnologias sejam utilizadas de forma ética e inclusiva.

Além de fomentar a regulação de tecnologias emergentes, este trabalho destaca a importância de investir na educação para a cidadania digital. A inclusão de temas como alfabetização digital e proteção de dados nos currículos escolares é essencial para formar cidadãos conscientes de seus direitos e deveres no ambiente digital. Paralelamente, é necessário

investigar o impacto das práticas de vigilância estatal e corporativa sobre a privacidade individual, especialmente em contextos de monitoramento em massa e reconhecimento facial.

Por fim, conclui-se que a efetivação do direito à privacidade digital e à proteção de dados pessoais exige uma reformulação profunda do paradigma normativo vigente. A regulação deve ser orientada por princípios dinâmicos e por uma governança adaptativa, baseada em riscos e respaldada por evidências. Este trabalho reafirma a necessidade de um sistema normativo que assegure a dignidade humana, a autodeterminação informacional e a justiça social em um ambiente digital em constante transformação.

Este estudo contribui, assim, para o avanço do debate jurídico e social, propondo soluções concretas e críticas às limitações atuais, servindo como base para futuros avanços legislativos, acadêmicos e institucionais.

REFERÊNCIAS

ABCOMM. **Previsão de vendas no e-commerce para os próximos 5 anos**. 2024. Disponível em: <https://dados.abcomm.org/previsao-de-vendas-online>. Acesso em: 10 de set. de 2024.

ABREU, Jacqueline de S. **Passado, presente e futuro da criptografia forte:** desenvolvimento tecnológico e regulação. Revista Brasileira de Políticas Públicas, Brasília, v. 7, n. 3, p. 24-42, 2017.

AGOSTINHO, Santo. **Confissões.** Trad. de Maria Luiza J. A. e revisão cortejada de acordo com o texto latino por António da Silveira Mendonça. São Paulo: Paulus, 1984.

ALBERTIN, Alberto Luiz. **Transformações digitais no comércio:** desafios e oportunidades. *In*: FGV. Relatório anual de comércio eletrônico 2022. São Paulo: FGV, 2022. Disponível em: <https://bibliotecadigital.fgv.br/dspace/handle/10438/31690>. Acesso em: 5 de set. de 2024.

ALBERS, Marion. **A complexidade da proteção de dados.** Revista Brasileira De Direitos Fundamentais & Justiça, v. 10, n. 35, p. 19-45, 2016.

AMARAL, João F. do. **Direito civil:** introdução. Rio de Janeiro: Renovar, 2008.

AMARAL, João F. do. **Economia da informação e do conhecimento**. Coimbra: Almedina, 2009.

ARENDT, Hannah. **A condição humana.** Trad. de Roberto Raposo e posfácio de Celso Lafer. 10. ed. Rio de Janeiro: Forense, 2007.

ÁVILA, Flávia; BIANCHI, Ana Maria. **Guia de economia comportamental e experimental.**São Paulo: Economia Comportamental. 2015.

BALKIN, Jack M. **Free speech is a triangle. Rochester**. NY: Social Science Research Network, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3186205>. Acesso em: 10 ago. 2024.

BARRETO JÚNIOR, Irineu F.; NASPOLINI, Samyra H.dal F. **Proteção de informações no mundo virtual:** a LGPD e a determinação de consentimento do titular para tratamento de dados pessoais. *In*: CZYMMECK, Anja (ed.). Proteção de dados pessoais: privacidade versus avanço tecnológico. 3. ed. Rio de Janeiro: Cadernos Adenauer, 2019. Cap. 7. p. 137-155.

BANDEIRA DE MELLO, Celso Antônio. **O conteúdo do princípio da igualdade.**São Paulo: Malheiros, 2009.

BANDURA, Albert. **Social learning theory**. New York: General Learning Press, 1977.

BAUMANN, Zygmunt. **Modernidade líquida.** Trad. de Plínio Dentzien. Rio de Janeiro: Jorge Zahar, 2001.

BERLIN, Isaiah. **Estudos sobre a humanidade:** uma antologia de ensaios. Trad. de Rosaura Eichenberg. São Paulo: Companhia Das Letras, 2002.

BIONI, Bruno Ricardo. **Autodeterminação informacional:** paradigmas inconclusos entre a tutela dos direitos da personalidade, a regulação dos bancos de dados eletrônicos e a arquitetura da internet. Dissertação (Mestrado) – Faculdade de Direito, USP, São Paulo, 2016.

BIONI, Bruno Ricardo. **Proteção de dados pessoais:**a função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo (org.). **Proteção de dados:** contexto, narrativas e elementos fundantes. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2022. PDF.

BIONI, Bruno Ricardo; ZANATTA, Rafael A. F. **Direito e economia política dos dados:** um guia introdutório. pp. 122-166. In: DOWBOR, Ladislau (org.). Sociedade vigiada: como a invasão da privacidade por grandes corporações e estados autoritários ameaça instalar uma nova distopia. São Paulo: Autonomia Literária, 2020.

BOBBIO, Norberto*et al*. **Dicionário de política.**2. vol. Brasília: Universidade de Brasília, 2004.

BOBBIO, Norberto. **Teoria do ordenamento jurídico**. 10. ed. Brasília: Editora UNB, 1995.

BORGES, Carolina Rego. **Herança digital:** a (in)suficiência das regras legais e a capacidade de autorregulação pelas plataformas digitais. 2024. 94 f., Dissertação (Mestrado em Direito, Regulação e Políticas Públicas) — Universidade de Brasília, Brasília, 2024.

BRASIL. *Constituição*. **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal, 1988.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018)**. Brasília: Planalto, 2018.

BRASIL. Ministério da Agricultura, Pecuária e Abastecimento. **Balança comercial do agronegócio 2023.** Disponível em: <https://www.gov.br/agricultura>. Acesso em: 16 de out. de 2024.

BRITO, Dante P. de; SILVA, Carlos M. M. da. **A publicidade nas redes sociais e seus impactos na cultura do consumismo**. Revista Jurídica Cesumar, v. 20, n. 1, p. 89-101, jan./abr. 2020.

BULOS, Uadi L. **Curso de direito constitucional**. São Paulo: Saraiva, 2008.

BURCH, Sally. **Sociedade da informação/sociedade do conhecimento**. Desafios de Palavras: Enfoques Multiculturais sobre as Sociedades da Informação. São Paulo: C&F editions, 2005.

CARNEIRO, Flávio L. **Fragmentação internacional da produção e cadeias globais de valor**. Texto para discussão, n. 2097. Brasília: Instituto de Pesquisa Econômica Aplicada, jun. 2015.

CARVALHO, Ana Paula V.; NEGÓCIO, Ramon de V. **A autorregulação regulada e a moderação de conteúdo no Facebook**. Revista de Direito, Governança e Novas Tecnologias, v. 9, n. 2, 2023.

CARVALHO, Orlando de. **Teoria geral do direito civil**. Coimbra: Coimbra Editora, 2012.

CASAGRANDE, Cledes Antônio. **Interacionismo simbólico, formação do "*self*" e educação:** uma aproximação ao pensamento de G. H. Mead. Educação e Filosofia, Uberlândia, v. 30, n. 59, p. 375–403, 2016.

CASTELLS, Manuel. **A galáxia da internet:** reflexões sobre a internet, os negócios e a sociedade. Trad. de Maria Luiza X. de A. B. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. **A sociedade em rede**. 1. vol. 6. ed. Trad. de Roneide V. Majer, com a colaboração de Klauss B.Gerhardt. São Paulo: Paz e Terra, 2002.

CASTELLS, Manuel; CARDOSO, Gustavo (org.). **A sociedade em rede:** do conhecimento a ação política. Conferência nacional promovida pelo Presidente da República de Portugal. Centro Cultural de Belém, 2005.

COHEN, Julie. ***Examined lives:*** *informational privacy and subject as object.*Stanford Law Review, n. 52, p. 1373-1438, 2000.

CORRÊA, Gustavo T. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 1999.

CUPIS, Adriano de. *Os direitos da personalidade***.** Trad. de Afonso Celso F. Rezende. São Paulo: Quórum, 2008.

CRUZ, Eduardo O. *et al*. **Coleta, utilização indevida e proteção de dados no ambiente digital na legislação brasileira:** a internet das coisas como sistema de transferência de dados pessoais.2024.

CUSTERS, Bart *et al*. ***Eu personal data protection in policy and practice*.**The Hague, The Netherlands: TMC Asser Press, 2019.

DANTAS, Marcos. **Capitalismo na era das redes:** trabalho, informação e valor no ciclo da comunicação produtiva. *Informação e globalização na era do conhecimento*. Rio de Janeiro: Campus, p. 216-261, 1999.

DASTIN, Jeffrey. **Amazon scraps secret AI recruiting tool that showed bias against women.**Reuters, 10 de out. de 2018. Disponível em: <https://www.reuters.com/article/usamazon-com-jobs-automationinsight/amazon-scraps-secret-ai-recruiting-tool-thatshowed-bias-against-women-idUSKCN1MK08G>. Acesso em: 02 de out. de 2024.

DATE. C. J. **Introdução a sistemas de bancos de dados**. 8. ed. Rio de Janeiro: Elsevier, 2003.

DE ARAÚJO, Luiz E. B.; CAVALHEIRO, Larissa N. **A proteção de dados pessoais na sociedade informacional brasileira:** o direito fundamental à privacidade entre a autorregulação das empresas e a regulação protetiva do internauta. Revista do Direito Público, v. 9, n. 1, p. 209-226, 2014.

DE SOUZA, Francielle Bertoncello P. **Direitos da personalidade:** uma nova categoria de direitos a ser tutelada. Dissertação (Mestrado). Direito. Faculdade de Maringá, 2006.

DE SOUZA, Jussara Feitosa. **Privacidade e dados pessoais:**o debate ético sobre o uso de big data. Revista Ilustração, v. 5, n. 6, p. 27-51, 2024.

DE SOUZA, Rosilene P. M.; SILVA, Paulo Henrique T. **Proteção de dados pessoais e os contornos da autodeterminação informativa**. Informação & Sociedade, v. 30, n. 2, 2020.

DE SOUZA SANTOS, Mário Filipe C. **Para além de um consentimento *naife*:** uma perspectiva analítica crítica do "consentimento" estampado na LGPD brasileira. Revista Jurídica da Seção Judiciária de Pernambuco, n. 15, p. 303-323, 2023.

DICIONÁRIO BRASILEIRO DA LÍNGUA PORTUGUESA. v. 3. São Paulo: *EncyclopaediaBritannica* do Brasil, 1987.

DONEDA, Danilo. **A proteção de dados pessoais como um direito fundamental**. Espaço Jurídico, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

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

DONEDA, Danilo **Princípios de proteção de dados pessoais**. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia R. P. Direito e Internet III: Marco Civil da Internet III–tomo II. São Paulo: Quartier Latin, p. 369-384, 2015.

DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel.**Estudos sobre proteção de dados pessoais:** direito, tecnologia, inovação e proteção de dados num mundo em transformação. Expressa, 2022.

DOMINGOS, Pedro. **O algoritmo mestre:** como a busca pelo algoritmo de machine learning definitivo recriará nosso mundo. Novatec Editora, 2017.

DOZZA, Eleonora C. **Uso secundário de dados pessoais e seu fundamento no legítimo interesse no Brasil pós-LGPD**. 2023.

DRUKER, Peter. **A sociedade pós-capitalista**. Trad. de Nivaldo M. Jr. São Paulo: Pioneira, 1993.

FEDERAL TRADE COMMISSION. **Data Brokers**. A call for transparency and accountability.Disponível em: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-reportfederal-trade-commission-may 2014/140527databrokerreport.pdf>. Acesso em 09 de set. 2024.

FELIPE, Patrícia L. **Mídias sociais, tecnologia persuasiva e a autonomia do consumidor na sociedade da sedução**. 2023.

FERRAZ JÚNIOR, Tércio S. **Introdução ao estudo do direito:**técnica, decisão, dominação. 4. ed. São Paulo: Atlas, 2003.

FERREIRA, Daniela A. A.; PINHEIRO, Marta M. Kerr; MARQUES, Rodrigo M. **Privacidade e proteção de dados pessoais:** perspectiva histórica. In: Revista de Ciência da Informação e Documentação, v. 12, n. 2, p. 151-172, 2021.

FRANÇA, Lilian Cristina M. **Vigilância e políticas de privacidade na sociedade pós cookie:** o caso do The Guardian. Revista Eco Pós, v. 18, n. 2, p. 95-105, 2015.

FRAZÃO, Ana. **A indústria dos dados pessoais e os data brokers.** Jota, 2019. Disponível em: <https://www. jota. info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/a-industria-dos-dados-pessoais-e-os-data-brokers-20032019> Acesso em: 17 de nov. de 2024.

FRAZÃO, Ana. **Data-driveneconomy e seus impactos sobre os direitos de personalidade**. Jota, v. 17, 2018.

FRAZÃO, Ana; CARVALHO, Ângelo G. P. de. **Os gigantes da internet e a apropriação e exploração de dados pessoais: direitos** fundamentais e direito ao esquecimento digital.*In*: A efetividade do direito em face do poder dos gigantes da internet: diálogos acadêmicos entre o Brasil e a França, v. 1, p. 303-342, 2018.

FRAZÃO, Ana; OLIVA, Milena D.; TEPEDINO, Gustavo (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de Direito Civil, v. 3***:* Responsabilidade Civil. 17. ed. São Paulo: Saraiva Educação, 2019.

GARCIA, Rafael Scaroni. **A mercadoria é você:** o uso secundário de dados pessoais.TCC em Bacharel em Ciências Jurídicas e Sociais pela UFRS, Porto Alegre, 2020.

GLEZER, Raquel. **Tempo e história.** Ciência e cultura, v. 54, n. 2, 2002.

GÓES, Bárbara V. et al. **Responsabilidade civil no descumprimento da nova lei geral de Proteção de Dados Pessoais (Lei No 13.709/2018)**. *In*: COSTA, Diego C. A discriminação algorítmica e as novas perspectivas sobre o tratamento de dados pessoais sensíveis. Proteção de

dados pessoais: novas perspectivas. Salvador: Editora da Universidade Federal da Bahia, 2021.

GOMES, Orlando. **Contratos de adesão:** condições gerais dos contratos. São Paulo: Revista dos Tribunais, 1972.

GOMES, Orlando. **Novos temas de Direito Civil.** Rio de Janeiro: Forense, 1983.

GREENWALD, G. ***NSA collecting phone records of millions of Verizon customers daily***. The Guardian. 6 jun. 2013.

GUIMARÃES, D. T. (org.). **Dicionário Técnico Jurídico.** São Paulo: Rideel, 1995.

HARARI, Yuval. N. **21 Lições para o Século 21**. São Paulo: Companhia das Letras, 2018.

HAN, Byung-Chul. **Sociedade da transparência**. Trad. de Ênio Paulo G. Petrópolis: Vozes, 2016.

HOBBES, Thomas. **Leviatã**. Org. de Richard T. Trad. de João Paulo M., Maria Beatriz N. da Silva e Claudia Berliner. Revisão da tradução de Eunice Ostrensky. Ed. brasileira supervisionada por Eunice Ostrensky. São Paulo: Martins Fontes, 2003.

HOFFMANN-RIEM, Wolfgang. **Autorregulação, autorregulamentação regulamentada no contexto digital.** Trad. de Luís Marcos Sander. Revista da AJURIS, Porto Alegre, v. 46, n. 146, junho/2019, p. 529-553.

HOUAISS, Antônio; VILLAR, Mauro de S. **Dicionário Houaiss da Língua Portuguesa**. Rio de Janeiro: Objetiva, 2009.

JOAQUIM, Rui Mateus. **Homo on-line***:* instruções neuropsicológicas na era das redes sociais. 1. ed. São Paulo: Vetor, 2021.

KANT, Immanuel. **A metafísica dos costumes**. Trad. de Edson Bini. 2. ed. Bauru: Edipro, 2008.

KOERNER, Andrei. **Capitalismo e vigilância digital na sociedade democrática**. Revista Brasileira de Ciências Sociais, v. 36, n. 105, 2021. Disponível em: <https://doi.org/10.1590/3610514/2020>. Acesso em: 04 de nov. de 2024.

KOTLER, Philip. **Princípios de marketing**. 10. ed. São Paulo: Prentice Hall, 2000.

KOTLER, Philip. ***Marketing insights from a to z:*** *80 concepts every manager needs to know. John Wiley & Sons, 2003.*

KOTLER, Philip; KELLER, Kevin L. **Marketing management**. Pearson Education. 14. ed. 2012.

KRIEGER, Matheus. **A evolução das normas de proteção de dados na União Europeia**. 2019.

LAFER, Celso.**A reconstrução dos direitos humanos:** um diálogo com o pensamento de Hannah Arendt. São Paulo: Companhia das Letras, 2005.

LE GOFF, Jacques. **A civilização do ocidente medieval**. Trad. de José R. de Macedo. Bauru, SP: Edusc, 2005.

LEHFELD, Lucas de S. *et al*. **A hipervulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD**. Revista Eletrônica Pesquiseduca, v. 13, n. 29, p. 236-255, 2021.

LEMOS, Ronaldo. **Uma nova lei para assegurar direitos na internet no Brasil:** o Marco Civil. Propriedades intelectuais, n. 2, 2014.

LIMA, Alminias da S. **Proteção de dados e consentimento:** limitações e desafios para o direito brasileiro. 2023.

LIMA, Cíntia R. Pereira de. **Os contratos de adesão eletrônicos (Shrink-Wrap e Clickwrap) e os termos e condições (Browse-Wrap)**. *In*: LIMA, Cíntia Rosa Pereira.; NUNES, Lydia N. B. Telles (coords.) Estudos avançados em direito digital. Rio de Janeiro: Elsevier, 2014.

LISBOA, Roberto S. **Direito na sociedade de informação**. Revista dos Tribunais, São Paulo, ano 1995, v. 847, p. 78-95, maio 2006.

LOPES, Juarez R. Brandão. **Sociedade industrial no Brasil**. Rio de Janeiro: Centro Edelstein de Pesquisas Sociais, 2008.

LORENZON, Laila N. **Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia (LGPD e GDPR) e seus respectivos instrumentos de enforcement**. Revista do Programa de Direito da União Europeia, v. 1, p. 39-52, 2021.

LUGATI, Lys N.; DE ALMEIDA, Juliana E. **Da evolução das legislações sobre proteção de dados:** a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. Revista de Direito, v. 12, n. 02, p. 01-33, 2020.

MAGRANI, E.**A internet das coisas.** Rio de Janeiro: FGV Editora, 2018.

MAGRO, Américo Ribeiro. **A autorregulação (regulada) das comunidades virtuais:**fundamentos, fatores e instrumentos autorregulatórios. 2020.

MALDONADO, Viviane N. **Avisos de privacidade e legal design**. *In*: OPICE BLUM, Renato. Proteção de Dados. São Paulo: Forense, 2020.

MAROTTA-WURGLER, Florencia. ***Will increased disclosure help?*** *Evaluating the recommendations of the ALI's principles of the law of software contracts*. U. Chi. L. Rev., v. 78, p. 165-186, 2011.

MARQUES, Claudia Lima.**Contratos no código de defesa do consumidor:** o novo regime das relações contratuais. São Paulo: Revista dos Tribunais, 2011.

MARTINS, Alexandre M. da S. **Os valores em Miguel Reale.** Revista de Informação Legislativa, Brasília: Senado Federal, serviço de informação legislativa, v. 45, n. 180, p. 263–277, out./dez. 2008.

MARTON, Scarlett. **O eterno retorno do mesmo:**tese cosmológica ou imperativo ético. *In*: Extravagâncias. São Paulo/Ijuí: Discurso/Unijuí, 2000.

MASUDA, Yoneji. ***The information society as post-industrial society***. Washington, D.C.: World Future Society, 1980.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. ***Big data:*** *a revolution that will transform how we live, work, and think.* First Mariner Books: New York, 2014.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data:** como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana; tradução Paulo Polzonoff Junior. 1º ed., Rio de Janeiro: Elsevier, 2013.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. ***General development of data protection in Europe****.In*: AGRE, Philip E.; ROTENBERG, Marc (org.). Technology and Privacy: The New Landscape. Cambridge: The MIT Press, p. 219-242, 1997

MEAD, George H. ***Mind, self, and society:*** *from the standpoint of a social behaviorist*. Chicago: University of Chicago Press, 1934.

MENDES, Laura Schertel; DA FONSECA, Gabriel C. S. **Proteção de dados para além do consentimento:**tendências contemporâneas de materialização. Revista Estudos Institucionais, v. 6, n. 2, p. 507-533, maio/ago. 2020.

MENDES, Laura Schertel. **O direito fundamental à proteção de dados pessoais**. Revista de Direito do Consumidor, v. 20, n. 79, p. 45-81, 2011.

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

MENDES, Laura Schertel. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. 2008.

MOHRI, Mehryar; ROSTAMIZADEH, Afshin; TALWALKAR, Ameet. ***Foundation of machine learning***. 2. ed. Cambridge MA: The MIT Press, 2018.

MONTEIRO, Renato L.**Existe um direito à explicação na Lei Geral de Proteção de Dados no Brasil?** Artigo Estratégico, Instituto Igarapé, dezembro de 2018.

MORATO, Antônio Carlos. **Quadro geral dos direitos da personalidade**. Revista da Faculdade de Direito da Universidade de São Paulo. v. 106-107, 2012.

MULHOLLAND, Caitlin Sampaio. **Dados pessoais sensíveis e a tutela de direitos fundamentais:**uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709/18). Revista de Direitos e Garantias Fundamentais, Vitória, v. 19, n. 3, 2018.

NERY, C. **Em 2023, 88,0% das pessoas com 10 anos ou mais utilizaram internet**. Agência: IBGE Notícias, 16 de agosto de 2024. Disponível em: <https://agenciadenoticias.ibge.gov.br>. Acesso em: 9 de set. de 2024.

NISSENBAUM, Helen. ***Privacyas contextualintegrity***. Washington Law Review, v. 79, p. 119- 158, 2004. Disponível em: <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10/>. Acesso em: 27/10/2024.

NISSENBAUM, Helen. ***Privacy in context:*** *technology, policy, and the integrity of social life*. Palo Alto: Stanford University Press, 2010.

NISSENBAUM, Helen; BARROCAS, Solon. ***On notice:*** *the trouble with notice and consent*. Proceedings of the engaging data forum: the first international forum on the application and management of personal electronic information, outubro de 2009.

NOGUEIRA, Magali G.; BIASI, Mario de. **Fontes e técnicas da cartografia medieval portulano.** Terra Brasilis (Nova Série) [online], Niterói, n. 4, p. 1-19, 2015. Disponível em: <https://journals.openedition.org/terrabrasilis/1240#abstract>. Acesso em 8 set. 2024.

NOJIRI, Sérgio. **O direito à privacidade na era da informática:** algumas considerações. Jur. UNIJUS, Uberaba/MG, v. 8, n. 8, maio de 2005.

ORWELL, George. **1984.** Trad. de Debora Fleck. São Paulo: LeYa Brasil, 2021.

O'NEIL, Cathy. ***Weapons of math destruction:*** *how big data increases inequality and threatens democracy*. Londres: Penguin Books, 2017.

PAESANI, Liliana M. (Coord.). **O direito na sociedade da informação**. São Paulo: Atlas, 2007.

PARISER, Eli. **O filtro invisível:** o que a internet está escondendo de você. Trad. Diego Alfaro. Rio de Janeiro: Zahar, 2012.

PRAZERES, Gustavo C. **Autodeterminação informacional vs. regulação do risco:** uma abordagem sistêmica da regulamentação digital. Revista Direito e Práxis, v. 13, p. 808-829, 2022.

POLANYI, Karl. **A grande transformação:** das origens à nossa época. Trad. de Fanny Wrabel. 2. ed. Rio de Janeiro: Compus, 2000.

POLČÁK, Radim; KASL, František; MÍŠEK, Jakub. ***National Report:*** *Czech Republic*. Data protection in the internet. p. 115-158, 2020.

RAMOS, Pedro. **A regulação de proteção de dados e seu impacto para a publicidade online:** um guia para a LGPD. v. 16, n. 07, 2019.

REALE, Miguel. **Filosofia do direito**. 20 ed. São Paulo: Saraiva, 2002.

REALE, M. **O estado democrático de direito e o conflito das ideologias.** São Paulo: Saraiva, 2005.

REINALDO FILHO, Demócrito. **A Diretiva Europeia sobre proteção de dados pessoais:** uma análise de seus aspectos gerais. Lex Magister, 2013.

RODRIGUES, Silvio. **Direito civil:** dos contratos e das declarações unilaterais de vontade. 30. ed. São Paulo: Saraiva. v. 3, 2004.

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

RODOTÀ, Stefano. ***Il dirittodiavere***. Roma: Laterza, 2012.

ROMERO, Luiz. **Não li e concordo**. 2017. Disponível em: <https://super.abril.com.br/tecnologia/naoli-e-concordo/>. Acesso em: 22 de nov. de 2018.

RUBINSTEIN, I. ***Technology and privacy by design***. Brooklyn Law School Research Papers, v. 12, 2011.

RYNGELBLUM, Ivan.**Nike vende operações na Argentina, Chile e Uruguai para o Grupo Axo**. Valor Econômico, publicado em 6 de fevereiro de 2020. Disponível em: <https://valor.globo.com/empresas/noticia/2020/02/06/nike-vende-operaes-na-argentina-chile-e-uruguai-para-grupo-axo.ghtml>. Acesso em: 18 de out. de 2024.

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

SENRA, Ricardo. **Dilema das redes:** os 5 segredos dos donos de redes sociais para viciar e manipular. Portal BBC News Brasil, Londres, 01 out. 2020. Disponível em: <https://www.bbc.com/portuguese/geral-54366416>. Acesso em: 04 de nov. de 2024.

SILVA, Daniel P. M. da. **Desafios do ensino jurídico na pós-modernidade:** da sociedade agrícola e industrial para a sociedade da informação. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica de São Paulo, São Paulo, 2009.

SILVA, Raphael F. S. **Igualdade e governança de redes sociais:** interseção entre tecnologia, moderação de conteúdo e direito à igualdade. Dissertação (Mestrado) - Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, Rio de Janeiro, 2022.

SILVA, Rosane L. da. **As tecnologias da informação e comunicação e a proteção de dados pessoais.***In*: Anais do XIX Encontro Nacional do CONPEDI. Fortaleza, 2010.

SIQUEIRA, OniyeNashara*et al*. **A (hiper) vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD**. RevistaEletrônicaPesquiseduca, v. 13, n. 29, p. 236-255, 2021.

SMITH, Huston. ***The world 's religions:*** *our great wisdom traditions*. New York: HarperSanFrancisco, 2009.

SOLOVE, Daniel J. ***A taxonomy of privacy*.** University of Pennsylvania law review**,** v. 154, n. 3, p. 477-560, 2006

SOLOVE, Daniel J. et al. ***The FTC the new common law of privacy***. *In*: 114 Columbia Law Review 583, 2014.

SOLOVE, Daniel J. ***Privacy Self-Management and the consent dilemma***. Harvard Law Review, v. 126, pp. 1880-1903, 2013.

SOLOVE, Daniel J. ***The digital person: technology and privacy in the information age.*** New York: NYU Press, 2004.

SOUSA, Rabindranath V. A. C. de. **O direito geral da personalidade**. Coimbra: Ed. Coimbra, 1995.

SOUZA, Thiago P. V. de. **A proteção de dados pessoais como direito fundamental e a incivilidade do uso de cookies.** Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Uberlândia, Uberlândia, 2018.

STRANDBURG, Katherine J. ***Free fall:*** *the online market's consumer preference disconnect.* NYU School of Law Research Paper, n. 13-34, p. 94-172, 2013. Disponível em: <https://ssrn.com/abstract=232396>. Acesso em 27 de nov. de 2024.

SZANIAWSKI, Elimar.**Direitos de personalidade e sua tutela.** São Paulo: RT, 2002.

TASSO, Fernando Antônio. **A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor**. Cadernos Jurídicos, São Paulo, v. 21, p. 97-115, 2020.

TEPEDINO, Gustavo.**Temas de direito civil**. 4. ed. Rio de Janeiro: Renovar, 2008.

TOBBIN, Raissa Arantes; CARDIN, Valéria S. G.**Política de cookies e a "crise do consentimento"***:* Lei Geral de Proteção de Dados e a autodeterminação informativa. Revista da Faculdade de Direito da UFRGS, n. 47, p. 241-262, 2021.

TONIAZZO, Daniela Wendt. **O consentimento na Lei Geral de Proteção de Dados e o problema da assimetria informacional:** soluções a partir da cláusula geral da boa-fé objetiva. Dissertação de Mestrado. Pontifícia Universidade Católica do Rio Grande do Sul, 2022.

UNIÃO EUROPEIA.**Regulamento Geral sobre a Proteção de Dados**. Artigo 4.º Definições. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 30 de set. de 2024.

VILLEY, Michel.**A formação do pensamento jurídico moderno**. Trad. de Claudia Berliner. São Paulo: Martins Fontes, 2005.

WAMBIER, Teresa A. A. **Uma reflexão sobre as "cláusulas gerais" do Código Civil de 2002:** a função social do contrato. Revista dos Tribunais. São Paulo, n. 831, janeiro de 2005.

WEISER, Mark. **The computer for the twenty-first century**. Scientific American. p. 94-100, 1991.

WIEACKER, Franz. **História do direito privado moderno.** Trad. de Antônio Manuel B. Espanha. Lisboa: Fundação Calouste Gulbenkian, 2004.

WOOD, David M.; MONAHAN, Torin. ***Platform surveillance.*** Surveillance & Society, v. 17, n. 1/2, p. 01-06, 2019.

ZANINI, Leonardo E. de A.**Direitos da personalidade:** aspectos essenciais. São Paulo: Saraiva, 2011.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira de poder. Trad. de George Schlesinger. Rio de Janeiro: Intrínseca, 2021.

ZUBOFF, Shoshana. ***Big other:*** *surveillance capitalism and the prospects of an information civilization*. Journal of Information Technology, 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754>. Acesso em: 8 de set. de 2024.