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

Elis Cristina Nogueira Xavier

PRIVACIDADE E ALGORITMOS:
Implicações da IA no Direito à Explicação

Belo Horizonte
2024

Elis Cristina Nogueira Xavier

PRIVACIDADE E ALGORITMOS:
Implicações da IA no Direito à Explicação

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

Orientador: Prof. Dr. Leonardo de Macedo Poli.

Linha de pesquisa: Novos Paradigmas, Sujeitos e Direitos.

Belo Horizonte
2025

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Xavier, Elis Cristina Nogueira
X3p Privacidade e algoritmos: implicações da IA no direito à explicação / Elis Cristina Nogueira Xavier. Belo Horizonte, 2025.
143 f. : il.

Orientador: Leonardo de Macedo Poli

Dissertação (Mestrado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito

1. Brasil. Lei geral de proteção de dados (2018). 2. Inteligência artificial. 3. Processamento eletrônico de dados. 4. Proteção de dados pessoais. 5. Algoritmos. 6. Transparência - Legislação - Brasil. 7. Tomada de decisão - Automação. I. Poli, Leonardo de Macedo. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito. III. Título.

CDU: 342.721

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

Elis Cristina Nogueira Xavier

PRIVACIDADE E ALGORITMOS:

Implicações da IA no Direito à Explicação

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

Área de concentração: Democracia, Autonomia Privada e Regulação.

Prof. Dr. Leonardo Macedo Poli – PUC Minas (Orientador)

Prof.ª Dra. Danúbia Patrícia de Paiva – UFSB (Banca Examinadora)

Prof.ª Dra. Maria de Fátima Freire de Sá – PUC Minas (Banca Examinadora)

Belo Horizonte, 10 de abril de 2025.

Dedico a inúmeras cientistas cujos nomes foram subtraídos da história da ciência.

AGRADECIMENTOS

Dizem que o verdadeiro sucesso está na alegria de ter pessoas especiais com quem compartilhar nossas conquistas. E hoje, olhando para trás nesta jornada extraordinária, meu coração transborda de gratidão ao perceber quantas pessoas maravilhosas fizeram parte desta história. Se por acaso minha memória falhar em mencionar alguém, peço, desde já, que me perdoem - são tantos momentos e pessoas especiais que às vezes as palavras não conseguem abraçar todos.

Início agradecendo a Deus e Nossa Senhora, meus guias espirituais que iluminaram meu caminho nos momentos mais desafiadores. Foram eles que me deram a força necessária para persistir quando o cansaço tentava me fazer desistir!

Aos meus amados pais, Jorge e Adorani, vocês são verdadeiros heróis! Não apenas por terem dedicado suas vidas para garantir que seus três filhos chegassem à universidade, mas por serem exemplos vivos de como a educação pode transformar vidas. Como educadores, vocês me mostraram o poder transformador do conhecimento na vida de jovens e adolescentes. Seu amor e dedicação são minha maior inspiração!

Meus queridos irmãos, Silvio e Luís, vocês são presentes divinos em minha vida! Seu apoio incondicional e orgulho em cada conquista minha me fortaleceram imensamente. Especialmente durante o período em que precisamos nos revezar nos cuidados com nossa mãe durante seu tratamento - vocês foram extraordinários!

Ao meu orientador Leonardo Poli, sua confiança em mim e em minhas ideias foi fundamental. Sua orientação precisa e seu apoio constante fizeram toda a diferença nesta trajetória.

À minha família estendida, que abriu não apenas suas casas, mas seus corações para me acolher: minha querida Tia Maria, Soraia e Ilídio, cujo otimismo e carinho foram bálsamos nos momentos difíceis.

À Maria Tereza (Tete), minha companheira de aventuras! Nossos shows e viagens foram os melhores remédios contra a ansiedade e o tédio - você trouxe alegria aos meus dias mais pesados!

Às amigas do coração: Livia (Livinha), minha parceira desde os primeiros passos no jardim de infância - que privilégio ter sua amizade por tantos anos! Alessandra (Alezoca), que compreendeu com tanto carinho minhas ausências pelos estudos - sim, um dia riremos de tudo isso em Paris!

E por falar em Paris, como não mencionar minha querida Juliana Rufino (nega), confidente e conselheira desde os primeiros dias na faculdade de direito. Quantas histórias vivemos naquela UIT gelada! À Jessica (Jefs), parceira nos estudos e na busca por nossos sonhos - sua amizade é um presente!

Ao pessoal incrível do cross, verdadeiros anjos que me proporcionaram momentos de leveza e descontração: os skeels Jordano, Marcos, René, Anne, Dani, Rômulo, Cláudio, Carol e Gui; e a turma mais divertida da "fofoca" - Bernard (Sereia), Monique, Renata, Débora, Jeizi, Natalia, Clara e Nathan. Vocês foram meu refúgio quando precisei esquecer um pouco o direito!

Aos amigos que o trabalho me presenteou: Erilaine, Eduarda e Fernanda - vocês são provas de que as melhores amizades podem nascer nos lugares mais inesperados. À querida Fiama (Fi), seu entusiasmo e apoio foram combustível para minha jornada!

Um agradecimento especial à Angelis - você foi muito mais que socorro nos momentos de aperto, foi uma verdadeira companheira de sonhos desde antes do mestrado começar. Aos colegas preciosos do PPGD: Júlia, Jefferson, Ana Flávia, Mariana, e especialmente à Marina, que mesmo do outro lado do oceano compartilhou comigo as alegrias e desafios dos artigos, escritas e congressos.

Aos mestres que marcaram minha trajetória acadêmica: vocês são verdadeiras inspirações! Com carinho especial ao professor Giovanni, que mesmo distante mantém seu cuidado e atenção. Aos professores que me acolheram e guiaram neste processo de aprendizagem: Taísa Maria, Maria de Fatima (nossa querida Fatinha), Walsir e Adalberto - vocês são exemplos que levarei para sempre!

À extraordinária professora Cláudia Viegas, sua generosidade em compartilhar conhecimento, seus conselhos preciosos e orientações fizeram toda a diferença - minha eterna gratidão!

Por fim, mas não menos importante, meu agradecimento carinhoso a toda equipe do ITS Rio, que não apenas me deu espaço para apresentar meus estudos, mas enriqueceu imensamente minha jornada acadêmica com suas valiosas contribuições.

A todos vocês, meu coração transborda de gratidão e amor!

Com licença poética
Quando nasci um anjo esbelto,
desses que tocam trombeta, anunciou:
vai carregar bandeira.
Cargo muito pesado pra mulher,
esta espécie ainda envergonhada.
Aceito os subterfúgios que me cabem,
sem precisar mentir.
Não sou feia que não possa casar,
acho o Rio de Janeiro uma beleza e
ora sim, ora não, creio em parto sem dor.
Mas o que sinto escrevo. Cumpro a sina.
Inauguro linhagens, fundo reinos
— dor não é amargura.
Minha tristeza não tem pedigree,
já a minha vontade de alegria,
sua raiz vai ao meu mil avô.
Vai ser coxo na vida é maldição pra homem.
Mulher é desdobrável. Eu sou.
(Adélia Prado, 1993, p. 11).

RESUMO

Esta dissertação analisa o direito à explicação como instrumento fundamental para a proteção dos direitos dos titulares de dados no contexto das decisões automatizadas, examinando sua fundamentação legal, alcance e mecanismos de efetivação no ordenamento jurídico brasileiro. A investigação parte da premissa de que, diante da crescente implementação de sistemas de IA em processos decisórios automatizados, torna-se imperativa a existência de mecanismos que garantam transparência e *accountability* algorítmica. O estudo reconstrói a evolução histórica da proteção de dados no Brasil, desde as primeiras previsões no CDC até a consolidação de um marco regulatório mais abrangente com a LGPD. A análise comparativa entre o modelo europeu (GDPR) e o brasileiro (LGPD) permite identificar convergências e particularidades na abordagem regulatória do direito à explicação, evidenciando como a flexibilidade da norma brasileira, embora permita maior adaptabilidade às transformações tecnológicas, demanda uma interpretação sistemática e teleológica para sua implementação. A pesquisa examina o precedente paradigmático do Superior Tribunal de Justiça sobre sistemas de *credit scoring* (REsp nº 1.419.697/RS), que estabeleceu importantes parâmetros para o equilíbrio entre necessidades comerciais e proteção dos direitos dos titulares de dados. Este julgamento antecipou discussões posteriormente incorporadas pela LGPD, como transparência algorítmica e direito à explicação. No âmbito da responsabilidade civil, identifica-se uma necessária evolução dos conceitos tradicionais para abarcar as especificidades das decisões automatizadas. A investigação demonstra que a explicabilidade emerge não apenas como um direito do titular, mas também como um dever do controlador, configurando-se como elemento essencial para a determinação de responsabilidades e para a própria legitimidade dos sistemas automatizados. Conclui-se que a aplicação do direito à explicação depende da implementação coordenada de medidas técnicas e jurídicas, incluindo o desenvolvimento de sistemas tecnicamente explicáveis, a adoção de práticas de governança adequadas e o estabelecimento de mecanismos regulatórios que equilibrem transparência e inovação. O estudo contribui para o debate sobre a regulação da IA ao propor uma abordagem integrada que reconhece tanto as limitações técnicas quanto as exigências legais e éticas envolvidas na explicabilidade de sistemas automatizados.

Palavras-chave: Inteligência Artificial; Direito à Explicação; Proteção de Dados; Transparência Algorítmica; Responsabilidade Civil.

ABSTRACT

This dissertation analyzes the right to explanation as a fundamental instrument for protecting data subjects' rights in the context of automated decisions, examining its legal foundations, scope, and enforcement mechanisms within the Brazilian legal system. The investigation starts from the premise that, given the increasing implementation of AI systems in automated decision-making processes, mechanisms ensuring algorithmic transparency and accountability become imperative. The study reconstructs the historical evolution of data protection in Brazil, from its initial provisions in the Consumer Protection Code to the consolidation of a more comprehensive regulatory framework with the General Data Protection Law (LGPD). The comparative analysis between the European (GDPR) and Brazilian (LGPD) models identifies convergences and particularities in the regulatory approach to the right to explanation, showing how the flexibility of Brazilian legislation, while allowing greater adaptability to technological transformations, demands a systematic and teleological interpretation for its effective implementation. The research examines the paradigmatic precedent of the Superior Court of Justice regarding *credit scoring* systems (REsp nº 1.419.697/RS), which established important parameters for balancing commercial needs and data subjects' rights protection. This ruling anticipated discussions later incorporated by the LGPD, such as algorithmic transparency and the right to explanation. In the realm of civil liability, the study identifies a necessary evolution of traditional concepts to encompass the specificities of automated decisions. The investigation demonstrates that explainability emerges not only as a right of the data subject but also as a controller's duty, establishing itself as an essential element for determining responsibilities and the legitimacy of automated systems. The research concludes that the effectiveness of the right to explanation depends on the coordinated implementation of technical and legal measures, including the development of technically explainable systems, the adoption of adequate governance practices, and the establishment of regulatory mechanisms that balance transparency and innovation. The study contributes to the debate on Artificial Intelligence regulation by proposing an integrated approach that recognizes both the technical limitations and the legal and ethical requirements involved in the explainability of automated systems.

Keywords: Artificial Intelligence; Right to Explanation; Data Protection; Algorithmic Transparency; Civil Liability.

LISTAS DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

IA – Inteligência Artificial

LGPD - Lei Geral de Proteção de Dados

UE - União Europeia

ANPD - Autoridade Nacional de Proteção de Dados

STJ - Superior Tribunal de Justiça

CDC - Código de Defesa do Consumidor

IDEC - Instituto de Defesa de Consumidores

PROCON-SP - Programa de Proteção e Defesa do Consumidor de São Paulo

CF - Constituição Federal

IoT - Internet das Coisas

AI Act - Ato de IA da União Europeia

PL – Projeto de Lei

ART. - Artigo

ML – Machine Learning

STF – Supremo Tribunal Federal

PEC – Projeto de Emenda à Constituição

RIPD – Relatório de Impacto à Proteção de Dados

DNN – Rede Neural Profunda

GTA29 - Grupo de Trabalho do Artigo 29

IBGE – Instituto Brasileiro de Geografia e Estatística

CF – Constituição Federal

TICs - Tecnologias da Informação e Comunicação

COVID-19 - Doença que se manifesta em seres humanos após a infecção causada pelo vírus SARS-CoV-2

PEC - Proposta de Emenda à Constituição

CC – Código Civil

SUMÁRIO

1 INTRODUÇÃO

A crescente integração da IA em processos decisórios automatizados tem transformado significativamente as dinâmicas sociais, econômicas e jurídicas contemporâneas. Esta revolução tecnológica, embora promissora em termos de eficiência e inovação, traz consigo desafios substanciais, particularmente no que diz respeito à opacidade dos sistemas algorítmicos e suas implicações para os direitos fundamentais dos indivíduos.

A problemática central desta pesquisa emerge da tensão entre a complexidade técnica dos sistemas de IA e a necessidade de transparência em suas decisões. Os algoritmos, especialmente aqueles baseados em aprendizado de máquina profundo (*deep learning*), frequentemente operam como "caixas-pretas", onde mesmo seus desenvolvedores encontram dificuldades para explicar precisamente como determinadas decisões são alcançadas. Esta opacidade torna-se especialmente preocupante quando tais sistemas são empregados em decisões que afetam direitos fundamentais, como avaliações de crédito, processos seletivos ou sistemas de vigilância.

A escolha do tema justifica-se pela crescente relevância da IA em processos decisórios que impactam diretamente a vida dos cidadãos. O potencial discriminatório de algoritmos opacos, evidenciado em casos como o reconhecimento facial errôneo em Sergipe e a discriminação algorítmica pela Amazon, demonstra a urgência de mecanismos que garantam transparência e responsabilização. Além disso, a recente evolução do marco regulatório de proteção de dados no Brasil, com a implementação da LGPD, torna oportuna e necessária a análise dos mecanismos de explicabilidade em sistemas automatizados.

O objetivo geral da pesquisa é analisar como o direito à explicação pode funcionar como instrumento de proteção dos direitos fundamentais no contexto das decisões automatizadas, investigando sua fundamentação legal, alcance e mecanismos de efetivação no ordenamento jurídico brasileiro. Os objetivos específicos compreendem examinar a evolução histórica e conceitual da IA e seus impactos nos direitos fundamentais, analisar o marco regulatório da proteção de dados pessoais no Brasil e sua relação com o direito à explicação, investigar os mecanismos técnicos e jurídicos disponíveis para promover a explicabilidade em sistemas de IA, e propor diretrizes para a implementação efetiva do direito à explicação no contexto brasileiro.

O trabalho estrutura-se em seis capítulos principais. Após esta introdução, o segundo capítulo aborda os desafios éticos e jurídicos da IA na era da vigilância digital, explorando como as tecnologias de monitoramento e análise de dados têm modificado as relações sociais e

jurídicas. O terceiro capítulo analisa a evolução do conceito de privacidade, desde a proteção passiva até a autodeterminação informativa, contextualizando as transformações conceituais necessárias para enfrentar os desafios contemporâneos. O quarto capítulo examina o perfilamento digital e suas implicações éticas e jurídicas, destacando como a análise preditiva de dados pessoais pode afetar direitos fundamentais. O quinto capítulo apresenta uma análise detalhada do direito à explicação no ordenamento jurídico brasileiro, explorando sua fundamentação legal e mecanismos de efetivação. Por fim, o sexto capítulo oferece as conclusões do estudo e perspectivas para o desenvolvimento futuro do tema.

A metodologia adotada é qualitativa e exploratória, baseada em pesquisa bibliográfica interdisciplinar e análise documental, abrangendo literatura jurídica e técnica, legislação nacional e comparada, jurisprudência e documentos técnicos relacionados à IA explicável. Esta abordagem permite uma compreensão abrangente do fenômeno estudado, considerando tanto seus aspectos jurídicos quanto técnicos.

Espera-se que esta pesquisa contribua para o debate sobre a regulação da IA no Brasil, oferecendo perspectivas para a implementação efetiva do direito à explicação e para o desenvolvimento de sistemas automatizados mais transparentes e responsáveis.

2 DESAFIOS ÉTICOS E JURÍDICOS DA IA NA ERA DA DATA VIGILÂNCIA

A crescente presença da IA[1] no cotidiano das sociedades contemporâneas tem se tornado um fenômeno inegável e de amplo alcance. Diariamente, os indivíduos são confrontados com uma miríade de aplicações dessa tecnologia, que vão desde recomendações personalizadas de produtos e conteúdos até sistemas complexos de reconhecimento facial e veículos autônomos. Esta onipresença da IA, que permeia tanto o setor público quanto o privado, tem suscitado reflexões profundas sobre os limites éticos de sua utilização e as possíveis consequências de sua implementação generalizada.

À medida que a IA se integra cada vez mais às rotinas diárias, cresce a consciência pública sobre o comportamento e as implicações desses sistemas inteligentes. Esta popularização não apenas evidencia o potencial transformador da tecnologia, mas também desperta preocupações[2], que abrangem desde questões de privacidade, vulnerável perante ao poder preditivo das grandes empresas de tecnologia, até o comprometimento de aspectos fundamentais da subjetividade humana, incluindo ainda os vieses discriminatórios com profundas implicações éticas (ROUVROY; BERNS, 2010).

Embora a IA ofereça um vasto potencial de aplicações, este trabalho foca especificamente nas situações onde as decisões são tomadas exclusivamente por sistemas automatizados e suas consequências. Inicialmente imperceptíveis, estas situações têm ganhado visibilidade midiática, expondo problemas éticos, jurídicos e sociais significativos.

Um exemplo contundente dessas implicações ocorreu em Sergipe, onde câmeras de reconhecimento facial com IA foram instaladas no Estádio de Futebol Arena Bastião, em

---

[1] Neste trabalho apresentaremos o conceito de IA, a fim de delimitar e esclarecer o tema. A IA geralmente é definida como a capacidade da máquina de interpretar dados de forma racional ou humana, tomando decisões autênticas com base em informações preexistentes. Fausto Santos Morais explica que o termo geralmente é constantemente empregado em um sentido amplo, abarcando quais programas computacionais aptos a reproduzir alguma habilidade humana. No entanto, estudos comportamentais têm sublinhado a presença de vieses cognitivos nas decisões humanas, levando muitos pesquisadores rejeitar a aptidão de 'pensar humanamente' como traço definidor da IA. Como resultado, parte expressiva da doutrina tem definido a IA como a capacidade da máquina de 'agir racionalmente'. Uma definição relevante para este trabalho é a formulada pelo autor John McCathy, reconhecido como o 'pai da IA', que define como a construção de um robô que se comporte de maneira que, caso se tratasse de um ser humano, fosse considerada inteligente. Em linhas gerais, pode-se representar pela "tentativa de reprodução da cognição humana e seus mais variados componentes – como o aprendizado, a memória e o processo de tomada de decisão – mediante o uso de softwares computacionais" (MORAIS, 2022; MCCARTHY, 2007; COSTA; NEGRI; DE OLIVEIRA, 2020, p. 85).

[2] A magnitude dessas preocupações é evidenciada por iniciativas como o consórcio formado em novembro de 2016 pelas cinco *big techs (*grandes empresas de tecnologia e inovação que apresentam dominância no mercado econômico. Destacam-se nomes como Google, Apple, Meta, Amazon e Microsoft) denominado *Partnership on AI to Benefit People and Societ*. Esta colaboração visa unificar conhecimentos e recursos, incorporando a governança de especialistas independentes em ética e outras áreas relevantes, para garantir uma perspectiva abrangente sobre o tema. Através de conferências, workshops e publicações, a parceria busca engajar formuladores de políticas e o público em discussões críticas sobre as implicações da IA.

Aracaju, com o propósito declarado de garantir a segurança dos torcedores. No entanto, em 13 de abril de 2024, um incidente envolvendo o personal trainer João Antônio Trindade Bastos expôs as falhas potenciais desse sistema. João Bastos foi erroneamente identificado, detido e conduzido algemado pelo gramado, diante de uma multidão, até ser liberado após insistente verificação de sua identidade (SERGIPE, 2024; FANTÁSTICO, 2024).

O incidente envolvendo o reconhecimento facial em Sergipe não é um caso isolado, mas sim um exemplo emblemático de uma tendência mais ampla na implementação de tecnologias de vigilância em todo o Brasil. Diante da repercussão midiática e do evidente constrangimento causado, o Governo Sergipano anunciou a suspensão do uso da tecnologia. Esta decisão veio após um investimento substancial de 87 milhões de reais na instalação de 800 câmeras em 81 municípios, operando ininterruptamente desde 2019, período no qual o sistema foi responsável pela prisão de 1.523 pessoas (UOL, 2024; SERGIPE, 2024).

Este episódio levanta questionamento sobre a eficácia e a ética do uso generalizado de sistemas de vigilância baseados em IA. Diversos estados brasileiros, incluindo Bahia, Rio de Janeiro e São Paulo, adotaram tecnologias similares, refletindo uma crença comum de que a vigilância contínua por câmeras é uma solução eficaz para identificar e erradicar a criminalidade. No entanto, o caso do personal trainer erroneamente detido em Sergipe sugere que estas tecnologias podem estar sujeitas a falhas significativas, com potenciais consequências graves para os direitos individuais e a justiça social.

É pertinente questionar quantos outros indivíduos podem ter sido vítimas de discriminação codificada sem que seus casos tenham recebido atenção nacional ou mesmo sido identificados. Este incidente expõe a ponta de um iceberg potencialmente vasto de injustiças algorítmicas.

O setor privado também não está imune a controvérsias semelhantes. Um exemplo notável ocorreu com o serviço Google Fotos, lançado em 2015. Esta plataforma, que utiliza IA para organizar e classificar fotos e vídeos, com *tags*[3], enfrentou um escândalo significativo quando um usuário negro descobriu que imagens suas e de uma amiga, também negra, foram categorizadas em uma pasta intitulada ‘Gorilas’. A resposta da empresa, expressando tristeza e constrangimento, e prometendo correções, sublinha a gravidade do problema e a necessidade de uma abordagem mais cuidadosa no desenvolvimento e implementação de sistemas de IA (LIMA; SÁ, 2020)

[3] Uma *tag*, ou em português etiqueta, é uma palavra-chave ou termo associado com uma informação que o descreve e permite uma classificação da informação baseada em palavras-chave (WIKIPÉDIA, 2024).

Estes casos suscitam uma série de questões éticas e jurídicas fundamentais sobre a IA abrangendo preocupações com a privacidade, o uso de algoritmos potencialmente discriminatórios e a capacidade das máquinas de reproduzir e amplificar preconceitos humanos. Além disso, evidenciam como a robótica está alterando profundamente as estruturas de relação social e os sistemas políticos.

As implicações dessas tecnologias se estendem até os processos democráticos e o pluralismo político. Marcos Antônio Sousa Alves e Marco Antônio Sousa Andrade alertam para os riscos de manipulação de imagem, disseminação de desinformação, radicalização ideológica e sofisticação das técnicas de censura e vigilância em massa. O que acarreta o seguinte questionamento: diante da opacidade destes sistemas e da incapacidade de compreender completamente seus processos decisórios, é prudente continuar delegando decisões tão impactantes a sistemas robóticos? (ALVES; ANDRADE, 2021)

É importante reconhecer que as decisões humanas também são influenciadas por concepções ideológicas, políticas, religiosas e sociais, frequentemente reproduzindo conceitos e preconceitos adquiridos ao longo da vida. No entanto, como Taísa Maria Macena de Lima e Maria de Fátima Freire de Sá apontam, não há garantia de que as decisões automatizadas, tomadas por sistemas ou robôs dotados de IA, sejam necessariamente mais precisas ou equânimes (LIMA; SÁ, 2020).

Para o usuário médio[4], os sistemas de IA frequentemente se apresentam como uma ‘cartola mágica’[5], cujo funcionamento interno permanece oculto, sendo apenas os resultados finais visíveis. Esta opacidade é muitas vezes justificada pela necessidade de proteger segredos industriais e propriedade intelectual, criando uma barreira significativa para a compreensão pública desses sistemas.

Quando questionados sobre o processo de tomada de decisão ou as razões por trás de sugestões específicas, os desenvolvedores de IA frequentemente recorrem a explicações que enfatizam a suposta neutralidade da tecnologia. Como apontado por Rafael Brandão *et al*., a resposta padrão muitas vezes se resume a: "Não sabemos explicar o modelo. Mas é difícil para nós explicar porque o modelo faz o que faz". Esta postura de aparente neutralidade e incompreensibilidade levanta questões significativas sobre responsabilidade e transparência (BRANDÃO *et al*, 2021, p.19).

---

[4] Neste documento utilizaremos a definição informal de ‘usuário médio’ como um usuário cujas características se encontram aproximadamente na média de todos os usuários. É um termo utilizado pelo design e pela programação.

[5] Utiliza-se a figura de linguagem da analogia para se referir ao instrumento pedagógico utilizado pelos profissionais da mágica.

A presente pesquisa reconhece que as soluções para os desafios éticos e políticos apresentados pela adoção generalizada de sistemas de IA transcendem o domínio puramente tecnológico. Portanto, propõe-se a examinar estes desafios através de uma lente multidisciplinar, abrangendo aspectos sociais e legislativos, com particular ênfase na responsabilidade civil e na explicabilidade dos sistemas de IA.

Em uma sociedade que busca progressivamente a inclusão e a equidade, evidenciada por legislações como a Lei Brasileira de Inclusão da Pessoa com Deficiência (Lei nº 13.146/15) e a equiparação da injúria racial ao crime de racismo (Lei nº 14.532/23), bem como por movimentos sociais como o combate ao capacitismo e o ciberativismo, se faz importante questionar a implementação de tecnologias que, sob o pretexto de neutralidade algorítmica, podem perpetuar ou exacerbar situações de preconceito e discriminação.

Embora o direito tenha recentemente despertado para os perigos do uso desenfreado da IA, outras disciplinas, incluindo a própria robótica, vêm abordando estas questões desde os primórdios do desenvolvimento da IA na década de 1960. As Três Leis da Robótica propostas por Isaac Asimov[6] em sua obra 'Eu, Robô', embora ficcionais, levantaram questões éticas fundamentais que continuam relevantes no debate contemporâneo sobre IA:

> 1ª Lei: Um robô não pode ferir um ser humano ou, por inação, permitir que um ser humano sofra algum mal.
> 2ª Lei: Um robô deve obedecer às ordens que lhe sejam dadas por seres humanos exceto nos casos em que tais ordens entrem em conflito com a Primeira Lei.
> 3ª Lei: Um robô deve proteger sua própria existência desde que tal proteção não entre em conflito com a Primeira ou Segunda Leis (ASIMOV, 2014, p. 41).

No entanto, à medida que avançamos para uma era de "data vigilância", surgem novos desafios que transcendem essas diretrizes iniciais. A coleta e análise massiva de dados pessoais por sistemas de IA suscita preocupações profundas sobre privacidade, segurança e liberdades individuais, tornando ainda mais urgente o debate sobre a regulamentação e a transparência dessas tecnologias.

O escopo desta dissertação concentra-se na análise crítica dos sistemas de IA e algoritmos decisórios que utilizam informações pessoais como base para seu treinamento e funcionamento. A pesquisa examina como esses mecanismos tecnológicos processam e aplicam dados individuais, bem como as consequências de sua implementação. Ao longo dos capítulos seguintes, será dada atenção especial às implicações desses sistemas para os direitos

[6] Isaac Asimov foi um escritor e bioquímico norte-americano, nascido na Rússia, autor de obras de ficção científica e divulgação científica. Asimov é considerado um dos mestres da ficção científica e, junto com Robert A. Heinlein e Arthur C. Clarke, foi considerado um dos "três grandes" dessa área da literatura.

fundamentais, com ênfase na salvaguarda de dados pessoais, na preservação da privacidade e na proteção da intimidade, tanto em nível individual quanto coletivo.

A crescente implementação de sistemas de IA e sua capacidade de processar volumes massivos de dados pessoais tem transformado fundamentalmente as dinâmicas de vigilância e controle social. Esta evolução tecnológica não apenas amplifica as capacidades de monitoramento existentes, mas também introduz novas formas de observação e análise comportamental que transcendem as limitações tradicionais de tempo e espaço. Para compreender adequadamente as implicações desta nova realidade tecnológica, é necessário primeiro examinar como a sociedade de vigilância se desenvolveu historicamente e quais são seus fundamentos estruturais. Esta análise nos permitirá contextualizar melhor os desafios contemporâneos que emergem da intersecção entre tecnologias de vigilância e direitos fundamentais, particularmente no que tange ao equilíbrio delicado entre segurança coletiva e privacidade individual.

2.1 A Sociedade de vigilância: entre a segurança e a privacidade

Desenvolvedores, programadores e o mercado propagam uma confiança na robótica que, paradoxalmente, não é acompanhada de uma compreensão profunda dos mecanismos subjacentes. Por exemplo, os motivos pelos quais um determinado filme é recomendado entre tantos outros permanecem obscuros até mesmo para os criadores dos sistemas. Esta opacidade, metaforicamente descrita como uma ‘caixa-preta’ por Zhang, não impede, contudo, a proliferação da confiança nesses sistemas (ZHANG; CHEN, 2020).

O prefácio de um robô, matemático, supostamente neutro, apolítico, distante dos problemas sociais atribuídos aos sistemas robóticos oferecem um conforto ilusório aos tomadores de decisão. Estes podem adotar posições sugeridas pelas máquinas sem reflexão crítica ou responsabilidade pelas consequências, reminiscente da postura dos agentes do Holocausto[7] que, durante os Julgamentos de Nuremberg, alegavam simplesmente ‘estar cumprindo ordens’.

[7] Holocausto foi o genocídio ou assassinato em massa de cerca de seis milhões de judeus durante a Segunda Guerra Mundial, o maior genocídio do século XX, através de um programa sistemático de extermínio étnico patrocinado pelo Estado nazista, liderado por Adolf Hitler e pelo Partido Nazista e que ocorreu em todo o Terceiro Reich e nos territórios ocupados pelos alemães durante a guerra. Dos nove milhões de judeus que residiam na Europa antes do Holocausto, cerca de dois terços foram mortos; mais de um milhão de crianças, dois milhões de mulheres e três milhões de homens judeus morreram durante o período.

Consolidou-se a crença generalizada de que a tecnologia oferece soluções para todos os problemas. Meredith Broussard denominou este fenômeno de 'tecnochavinismo', destacando como o entusiasmo em torno das inovações tecnológicas frequentemente ofusca a percepção dos problemas que estas podem gerar ou exacerbar (BROUSSARD, 2019).

Esta tendência evoca paralelismos com o pensamento dominante durante a Revolução Científica[8], período em que a exatidão era equacionada à matematização. Heidegger, alerta para os limites desta abordagem, especialmente quando aplicada a sistemas complexos como os organismos vivos:

> [...] se a possibilidade de matematização de uma ciência reside no conteúdo objetivo (Sachgehalt) e no modo de ser (Seinsart) do âmbito de objetos, então ainda se carece, além disso, da motivação inerente à necessidade de uma tal possibilidade. Assim, os seres vivos como corpos extensos admitem uma certa determinabilidade matemática, mas a realização ilimitada dessa possibilidade faria com que se falhasse no propósito de apreender e determinar o organismo como tal (HEIDEGGER, 1996, p. 43).

O fenômeno contemporâneo denominado '*mathwashing'*, ou 'lavagem matemática', refere-se à prática de ocultar as responsabilidades dos tomadores de decisão por trás da aparente objetividade da matemática e dos algoritmos. Esta prática contribui para a opacidade dos processos decisórios baseados em IA (BENENSON, 2021).

Com cada novo sistema de IA lançado no mercado, os indivíduos se submetem ao "risco de o crescimento da autonomia artificial minar o florescimento da autonomia humana". As pequenas conveniências oferecidas, como otimização do tráfego ou recomendações de entretenimento, vêm acompanhadas de vieses que tendem a favorecer certas perspectivas culturais em detrimento de outras, potencialmente marginalizando vozes minoritárias e produções regionais (FLORIDI, COWLS, 2019, p. 7).

Nesse sentido, os autores Nelson Rosenvald e Felipe Braga Netto alertam para a dualidade da tecnociência, que promete um futuro melhor para a humanidade, mas simultaneamente apresenta ameaças à própria sobrevivência humana, tornando o indivíduo extremamente vulnerável:

> A tecnociência possibilitou à ação humana o exercício de poderes que representam uma promessa de um futuro melhor para a humanidade, mas também se constituem

[8] Na história da ciência, chama-se Revolução da Científica ao período que começou no século XVI e prolongou-se até o século XVIII. Começou na era renascentista, na sequência deste espírito crítico. Os conhecimentos só eram considerados corretos depois de confirmados pela experiência e razão, surgindo assim o método experimental ou científico. A partir desse período, a Ciência, que até então estava atrelada à Teologia, separa-se desta e passa a ser um conhecimento mais estruturado e prático. As causas principais da revolução podem ser resumidas em: Renascimento cultural e científico, a imprensa, a Reforma Protestante e o hermetismo.

> em uma espada de Dâmocles, que ameaça a própria sobrevivência do homem. O ser humano tornou-se, então, extremamente vulnerável na sua individualidade e a única certeza que se tem é que, em longo prazo, toda ação gera efeitos ameaçadores (NETTO; ROSENVALD, 2024, p. 4).

Os sistemas de IA dependem fundamentalmente dos dados como matéria-prima para seu desenvolvimento. A eficácia do aprendizado, o grau de autonomia e o padrão comportamental desses sistemas estão diretamente vinculados à extensão e à qualidade dos dados processados durante sua fase de treinamento. Por exemplo, campo do aprendizado de máquina[9], é amplamente aceito que a excelência de um modelo está intrinsecamente ligada à qualidade dos dados que o alimentam. Em uma sociedade que anseia por mais segurança, emerge a chamada 'sociedade de vigilância'.

Na era atual, caracterizada pela crescente 'datificação'[10] da sociedade, praticamente todos os aspectos da vida humana são passíveis de serem convertidos em dados quantificáveis. Esse fenômeno amplia consideravelmente o escopo de temas sujeitos a análises algorítmicas probabilísticas, possibilitando novas formas de associação entre diferentes tipos de informação (MAYER-SCHÖNBERGER; CUKIER, 2013).

No âmbito da *big data*, o acúmulo massivo de informações em repositórios digitais tem como objetivo primordial a realização de análises preditivas e o estabelecimento de correlações. Isso é alcançado através do emprego de algoritmos avançados, visando subsidiar ou automatizar processos decisórios. Esse movimento é impulsionado por diversos fatores, incluindo o desenvolvimento de métodos estatísticos e probabilísticos cada vez mais sofisticados, a disponibilidade ampla e crescente de dados, o acesso a um poder computacional expressivo e econômico, e a transformação de espaços com novas tecnologias da informação, como

---

[9] O Aprendizado de Máquina (*Machine Learning* - ML) representa um subcampo crucial da IA, focado no desenvolvimento de algoritmos e modelos estatísticos que permitem que os sistemas de computador melhorem seu desempenho em uma tarefa específica através da experiência, sem serem explicitamente programados para cada cenário possível. Esta abordagem é particularmente poderosa em situações onde as regras tradicionais de programação seriam muito complexas ou impossíveis de serem definidas manualmente (MITCHELL, 2019).

[10] Para os autores Mayer-Schönberger e Cukier praticamente toda informação pode ser capturada e convertida em dados interpretáveis por sistemas computacionais, possibilitando análises posteriores. Este fenômeno resulta na mensuração quantitativa de uma vasta gama de atividades humanas, abrangendo desde preferências culturais e hábitos cotidianos até indicadores fisiológicos. Um aspecto notável deste cenário de abundância de dados é a versatilidade de sua aplicação. Informações originalmente coletadas com um propósito específico frequentemente encontram novas aplicações, muitas vezes em contextos completamente distintos do original. Surpreendentemente, essas análises secundárias e imprevistas têm demonstrado uma eficácia considerável, revelando insights valiosos que transcendem a intenção inicial da coleta de dados. Esta capacidade de reutilização e reinterpretação de dados em contextos diversos representa uma das características mais significativas e potencialmente transformadoras da atual revolução informacional. Ela abre caminho para descobertas inovadoras e aplicações inéditas, ao mesmo tempo em que suscita questões importantes sobre privacidade e ética no uso de informações pessoais (MAYER-SCHÖNBERGER; CUKIER; 2013, p. 97).

residências automatizadas e cidades inteligentes (COSTA; DE OLIVEIRA; NEGRI *apud* FLORIDI *et al*, 2020).

Esta evolução tecnológica possibilita associações inéditas entre diferentes tipos de informação, transcendendo as intenções originais de coleta de dados e revelando *insights* valiosos em contextos diversos. Contudo, essa capacidade de reutilização e reinterpretação de dados, embora promissora para inovações e descobertas, amplia a quantidade de preocupações como as anteriormente levantadas pelas do 'tecnochavinismo' e o 'mathwashing', criando o que a autora Ana Frazão descreve como "uma das fases de fenômeno mais abrangente e complexos, que diz respeito a uma sociedade movida a dados, a uma política movida a dados e às trajetórias pessoais dos indivíduos também movidas a dados" (FRAZÃO, 2019, p.34).

Consequentemente, a crença na neutralidade e infalibilidade desses sistemas pode levar a uma confiança excessiva em suas decisões, potencialmente agravando problemas sociais existentes ou criando novos.

A opacidade desses sistemas, frequentemente referida como 'caixa-preta' algorítmica, torna-se ainda mais problemática quando considerada a escala e o alcance da data vigilância contemporânea. Rodotà observa que a ascensão incontida da internet, acrescida de crescente e intensa coleta de dados pessoais e interconexão entre diversos bancos de dados, transformou a sociedade em uma pauta pelo controle, vigilância e classificação. O autor alerta que esta tendência "já parece irresistível, comum aos mais diversos países" (RODOTÀ, 2008, p. 147).

O interesse nas tecnologias emergentes de IA e análise de dados em larga escala é compartilhado tanto pelo setor público quanto pelo privado, cada um vislumbrando benefícios potenciais em suas respectivas esferas de atuação. Para os gestores públicos, estas tecnologias representam uma ferramenta poderosa para a otimização do planejamento urbano, permitindo uma compreensão mais profunda e dinâmica das necessidades e comportamentos dos cidadãos. Isso pode resultar em políticas públicas mais eficientes e direcionadas, melhorando a qualidade de vida nas cidades e a alocação de recursos públicos.

Por outro lado, o setor privado vê neste campo um vasto campo para o desenvolvimento de novas aplicações e a expansão de mercados. Um exemplo notável deste público é o crescimento exponencial da 'Internet das Coisas' (IoT)[11] que se interconecta com uma miríade

[11] IoT, do inglês *internet of thing*s, em tradução livre, Internet das Coisas. Este termo abrange a capacidade de diversos objetos do dia a dia de se comunicarem e interagirem através da internet. A IoT representa um ecossistema digital onde não apenas dispositivos, mas também indivíduos, informações e ambientes virtuais estão em constante interação, transcendendo barreiras espaciais e temporais. Esta rede interconectada de "coisas" inteligentes está redefinindo a forma como interagimos com nosso ambiente físico e digital. Esta integração tecnológica permeia diversos aspectos de nossas vidas, desde eletrodomésticos e veículos até

de dispositivos cotidianos na internet, gerando um volume sem precedentes de dados sobre o comportamento e as opiniões dos consumidores (COSTA; DE OLIVEIRA; NEGRI, 2020).

Esta convergência de interesses entre o público e o privado no uso de tecnologias de dados coloca a sociedade diante de um dilema fundamental: como equilibrar os benefícios potenciais da IA e a análise de dados em larga escala com a necessidade premente de proteger os direitos individuais, preservar a autonomia humana e garantir a equidade social em um mundo cada vez mais digitalizado e vigiado. Este desafio exige uma reflexão profunda e multidisciplinar, envolvendo não apenas aspectos técnicos, mas também considerações éticas, legais e sociais para garantir um desenvolvimento tecnológico responsável e benéfico para toda a sociedade.

As implicações dessas aplicações tecnológicas vão muito além da mera facilitação da comunicação, economia de tempo ou execução de funções específicas. Resultam em uma "coleta, transmissão, armazenamento e compartilhamento de dados entre os objetos e, consequentemente, entre as empresas que disponibilizam este tipo de tecnologia às pessoas". Este fluxo contínuo e muitas vezes invisível de informações pessoais importa em questionamentos sobre privacidade, segurança de dados e o controle que os indivíduos têm sobre suas informações (MULHOLLAND, 2019, p. 485-486).

No âmbito das tecnologias de IA, o reconhecimento facial tem se destacado como uma aplicação particularmente poderosa e controversa. Esta tecnologia se apresenta como uma solução para “superar a incapacidade do cérebro humano de processar, memorizar e lembrar-se de milhares de faces com que se depara todos os dias”. Sua capacidade de identificar e catalogar indivíduos em grandes volumes de dados visuais atraiu interesse significativo, especialmente no contexto de segurança pública e combate ao crime (COSTA; DE OLIVEIRA; NEGRI *apud* VU, 2018, p. 11-12).

A implementação de tecnologias que permitem a agilidade na análise dos dados ganhou impulso notável após os ataques terroristas de 11 de setembro de 2001[12] nos Estados Unidos. Este evento catalisou a adoção generalizada de tecnologias de vigilância, sob o argumento de

infraestruturas urbanas inteiras, criando um tecido digital que envolve nossa existência cotidiana (MAGRANI, 2018).

[12] Os ataques terroristas de 11 de setembro de 2001, realizados pela organização Al-Qaeda, envolveram o sequestro de quatro aviões nos Estados Unidos. Dois deles foram colididos contra as Torres Gêmeas em Nova York, levando ao desmoronamento dos prédios e à destruição de edifícios próximos. Um terceiro avião atingiu o Pentágono, e o quarto caiu em um campo na Pensilvânia após uma tentativa de retomada da aeronave pelos passageiros. No total, quase três mil pessoas morreram, incluindo os passageiros, tripulantes e os sequestradores. A maioria das vítimas eram civis de várias nacionalidades (GOUVEIA, 2023).

proteção da segurança nacional e prevenção de ameaças terroristas. Como assistido por Ramon Silva Costa, Sergio Marcos Carvalho Negri e Samuel Rodrigues De Oliveira:

> Porém, na atualidade, e especialmente, depois dos ataques terroristas ocorridos em setembro de 2001 nos EUA, agências governamentais têm-se utilizado de todos os meios para desenvolver maneiras eficientes e precisas de regular o afluxo de pessoas por meio de identificação dos indivíduos, a fim de garantir que nenhuma ameaça conhecida seja permitida, pois, argumenta-se, isso pode colocar em risco os cidadãos de uma sociedade (COSTA; NEGRI; DE OLIVEIRA *apud* VU, 2018, p. 11-12).

Essa tendência levou a uma limitação crescente da vigilância em massa em nome da segurança coletiva, levantando debates intensos sobre o equilíbrio entre a segurança pública e os direitos individuais à privacidade.

É crucial notar que os grandes bancos de dados que alimentam esses sistemas não são necessariamente "resultado de uma atividade deliberada e específica". Como observam Ramon Silva Costa, Sergio Marcos Carvalho Negri e Samuel Rodrigues De Oliveira, eles são frequentemente um subproduto do comportamento cotidiano das pessoas, que voluntariamente compartilham uma vasta quantidade de informações sobre si mesmas em troca de participação em comunidades virtuais ou acesso a serviços online. Esta dinâmica cria um cenário onde, nas palavras de Han, "o *big data* torna possível uma forma de controle muito eficiente" (COSTA; DE OLIVEIRA; NEGRI, 2020, p. 89; HAN, 2018b, p.78).

A natureza dessa vigilância é universal e abrangente, não expande o controle de indivíduos específicos, mas sim de toda a população. É importante ressaltar que este controle não é uma prerrogativa exclusiva dos órgãos de segurança; pelo contrário, ocorre predominantemente para fins comerciais. Esta realidade levanta questões importantes sobre a privacidade e a autonomia individual na era digital (COSTA; DE OLIVEIRA; NEGRI, 2020; RODOTÀ, 2013).

O filósofo sul-coreano Byung-Chul Han utiliza o termo 'pan-óptico'[13] para definir este período de "aparente liberdade e comunicação ilimitada", onde "a transparência e a informação substituem a verdade". Diferentemente do conceito original de panóptico de Bentham, treinado

[13] O termo "efeito pan-óptico" deriva do conceito de "Panóptico", uma estrutura arquitetônica projetada pelo filósofo e teórico social Jeremy Bentham no século XVIII. O Panóptico era uma prisão circular com uma torre de vigilância no centro, de modo que um único guarda pudesse observar todos os prisioneiros sem que estes soubessem quando estavam sendo observados. Esse design visava induzir uma sensação constante de vigilância nos prisioneiros, levando-os a se comportar como se estivessem sempre sob supervisão. O "efeito pan-óptico" refere-se à aplicação desse princípio de vigilância constante e invisível em contextos modernos, especialmente com a utilização de tecnologia. A ideia é que a mera possibilidade de ser observado leva as pessoas a regularem seu próprio comportamento. Este conceito é amplamente discutido em estudos sobre vigilância, privacidade e controle social, particularmente no contexto da sociedade digital contemporânea (HAN, 2018b).

por Foucault, no contexto digital atual, as pessoas não se sentem necessariamente vigiadas ou ameaçadas. Paradoxalmente, há um sentimento predominante de liberdade, mas Han argumenta que "é exatamente esse sentimento de liberdade, inexistente no Estado de vigilância de Orwell, que constitui um problema" (HAN, 2018b, p. 56 – 57).

Han elaborou esta ideia, afirmando que:

> o pan-óptico digital oferece uma visão em 360º dos seus internos. O pan-óptico de Bentham está ligado à óptica perspectiva. Desse modo, são inevitáveis pontos cegos nos quais os prisioneiros podem perseguir seus pensamentos e desejos secretos sem serem notados. A vigilância digital é mais eficiente porque é aperspectivista. Ela é livre de limitações perspectivas que são características da óptica analógica. A óptica digital possibilita a vigilância a partir de qualquer ângulo. Assim, elimina pontos cegos. Em contraste com a óptica analógica e perspectiva, a óptica digital pode espiar até a psique. (HAN, 2018b, p. 78).

Esta reflexão sobre a visão de dados e seus impactos na sociedade enfatiza que os novos modelos tecnológicos não são específicos naturais incontroláveis, mas criações humanas. Como seres sociais, nosso convívio com essas tecnologias é inovador, não se resumindo a uma simples escolha entre "aceitar e viver com ela" ou "rejeitar e viver sem ela". Neste contexto, Klaus Schwab argumenta pela necessidade de uma abordagem colaborativa:

> É, portanto, crucial que nossa atenção e energia estejam voltadas para a cooperação entre múltiplos stakeholders que envolvam e ultrapassem os limites acadêmicos, sociais, políticos, nacionais e industriais. As interações e as colaborações são necessárias para criarmos narrativas positivas, comuns e cheias de esperança que permitam que indivíduos e grupos de todas as partes do mundo participem e se beneficiem das transformações em curso. (SCHWAB, 2016, p. 14)

Esta transformação tecnológica representa uma oportunidade única para a sociedade refletir sobre os rumores aos quais está sendo fornecida, proporcionando uma chance de melhoria e redefinição de paradigmas. Stefano Rodotà argumenta que estes novos conceitos de vigilância permitem uma nova abordagem sobre a privacidade, reconhecendo a necessidade de adaptação dos marcos regulatórios e éticos frente às mudanças tecnológicas (NETTO; ROSENVALD, 2024; RODOTÀ, 2013).

A evolução das tecnologias de vigilância, especialmente após o advento das ferramentas digitais, transformou profundamente a dinâmica do monitoramento social. Se inicialmente a vigilância se caracterizava por estruturas físicas e hierarquias visíveis de poder, como no modelo pan-óptico tradicional, o cenário contemporâneo apresenta uma forma mais sutil e pervasiva de controle. Esta transição não é apenas tecnológica, mas representa uma mudança fundamental na própria natureza da vigilância, que agora se integra de maneira quase

imperceptível ao cotidiano digital. À medida que adentramos esta nova era, onde dados pessoais se tornam a principal moeda de troca nas interações sociais e comerciais, emerge a necessidade de compreender como esta transformação afeta não apenas nossa privacidade, mas também nossa autonomia e capacidade de autodeterminação no ambiente digital.

2.2 A Sociedade de Vigilância Digital: Desafios à Privacidade e a Autonomia na Era dos Dados

O desenvolvimento tecnológico não apenas altera os paradigmas legais, mas também, nas palavras de Stefano Rodotà possibilita que "os riscos da sociedade de vigilância ligam-se tradicionalmente ao uso político de informações para controlar os cidadãos", o que "implicam uma mudança na subjetividade das relações entre as pessoas e a tecnologia", reconhecendo que as implicações desta vigilância generalizada se estendem além do controle político, afetando profundamente a formação da personalidade e o exercício da autonomia privada (RODOTÀ, 2008, p.113; DONEDA *et al.*, 2018, p.2).

A onipresença do monitoramento na era digital é uma realidade inescapável, ocorrendo frequentemente sem a ciência ou consentimento explícito dos indivíduos. Como observa Clarisse Souza, o simples fato de existir na sociedade implica estar sujeito a uma vigilância constante, seja através de câmeras, sensores, monitoramento de dados produzidos em atividades cotidianas, ou pela presença quase obrigatória em redes sociais e uso de dispositivos conectados à IoT. Esta vigilância pode ser voluntária, quando os dados são cedidos de forma consciente, ou involuntária, resultando em uma vigilância ostensiva e muitas vezes imperceptível (SOUZA, 2018).

No mais, a complexidade das relações contratuais adiciona uma camada a este cenário. Para os autores Felipe Braga Netto e Nelson Rosenvald um simples clique (*click-wrap*) pode transformar contratos de adesão em leis entre as partes, frequentemente concedendo a grandes empresas direitos extensivos sobre dados pessoais sem um consentimento verdadeiramente informado. Este fenômeno reflete uma tendência mais ampla na qual o contrato, em muitos setores, substitui a lei no papel de organização da sociedade civil (NETTO; ROSENVALD *apud* GALGANO, 2024, p. 18).

O surgimento de uma 'nova *lex mercatoria*'[14], como apontado por Felipe Braga Netto e Nelson Rosenvald, representa um direito criado por empreendedores sem a mediação do poder legislativo estatal. Esta evolução busca soluções adequadas às expectativas do comércio internacional, operando independentemente dos sistemas jurídicos nacionais. Paradoxalmente, neste ambiente, a proteção do consumidor emerge como um diferencial competitivo, visando incrementar vendas, mas potencialmente mascarando questões mais profundas de autonomia e privacidade (NETTO; ROSENVALD, 2024).

A crescente especialização e personalização dos serviços, embora aparentemente benéfica, suscita preocupações significativas no que tange à privacidade e à autonomia privada dos indivíduos. Nelson Rosenvald e Felipe Braga Netto demonstram que para o risco de despersonalização neste processo, onde a aparente liberdade proporcionada pelo ciberespaço pode, na realidade, ocultar formas mais sutis e eficazes de controle social:

> [...] ilusão de livre-arbítrio proveniente da narrativa liberal provavelmente se desintegrará quando, mesmo em sociedades supostamente livres, deparamo-nos diariamente com instituições, corporações e agências governamentais que compreendem e manipulam o que até então era nosso inacessível reino interior (ROSENVALD; NETTO, 2024, p. 17).

Han aprofunda esta análise, propondo uma mudança paradigmática na compreensão do poder na era digital. Segundo o autor, transitamos de um modelo de biopoder, como descrito por Foucault, para um cenário de "transparência psicopolítica", ou seja, o "psicopoder" cuja a formula do sucesso tange a "possuir condições de intervir nos processos psicológicos", é uma espécie capacitada para "ler e controlar o pensamento, e, consequentemente, influenciar o comportamento das pessoas". Esta forma de poder, argumenta-se, é mais eficiente e pervasiva que o biopoder tradicional, pois opera de maneira mais requintado e internalizada (HAN, 2018a; COSTA; DE OLIVEIRA; NEGRI, 2020, p. 95).

> [...] o data-mining torna visíveis os modelos coletivos de comportamento dos quais não se está, enquanto indivíduo, nem sequer consciente. Assim, ele torna acessível o inconsciente-coletivo. Em analogia ao inconsciente-ótico, pode-se também chamá-lo de inconsciente-digital. O psicopoder é mais eficiente do que o biopoder na medida em que vigia, controla e influencia o ser humano não de fora, mas sim a partir de dentro. A psicopolítica se empodera do comportamento social das massas ao acessar a sua lógica inconsciente. A sociedade digital de vigilância, que tem acesso ao inconsciente-coletivo, ao comportamento social futuro das massas, desenvolve trações totalitários. Ela nos entrega à programação e ao controle psicopolítica. A era da biopolítica está, assim, terminada. Digirimo-nos, hoje, à era da psicopolítica digital (HAN, 2018a, p. 134).

[14] *Lex mercatória* significa um conjunto de procedimentos que possibilita adequadas soluções para as expectativas do comércio internacional, sem conexões necessárias com os sistemas nacionais e de forma juridicamente eficaz.

A evolução da IA, em particular, merece atenção especial devido à sua capacidade de influenciar a subjetividade da relação humana com a tecnologia. As novas formas de comunicação e informação moldadas por esta tecnologia impactam diretamente o modo como os indivíduos constroem suas visões sobre si mesmos e sobre o mundo, afetando o direito fundamental de construir livremente a própria esfera privada (DONEDA *et al*.,2008).

James Beniger oferece uma perspectiva histórica ao afirmar que "[c]ada nova inovação tecnológica estende os processos que sustentam a vida social humana, aumentando assim a necessidade de controle e a melhoria da tecnologia de controle". Esta observação ressoa com a metáfora do *one-way mirror*[15] proposta por Filipe Medon, que descreve uma realidade onde um lado detém o poder de observação total, enquanto o outro permanece na obscuridade (BENIGER, 1986, p.434; MEDON, 2020).

A evolução dos sistemas de vigilância e controle social evidencia uma transformação paradigmática que transcende o modelo presencial e moralmente complexo proposto por Bentham e Foucault, culminando no que Han denomina pan-óptico digital. Este novo sistema, fundamentalmente mais eficiente que seu predecessor benthamiano, caracteriza-se pela capacidade de armazenamento e análise abrangente das ações humanas, superando limitações espaciotemporais. Esta transição representa uma mudança significativa na natureza do controle social, onde, conforme Lianos e Douglas, abandona-se um sistema tradicionalmente negociado e dotado de função moral-educativa, que demonstrava e reforçava valores sociais, em favor de uma abordagem tecnológica mais binária e reducionista, operando sob critérios simplificados e frequentemente opacos (HAN, 2018b; LIANOS; DOUGLAS *apud* NORRIS, 2003).

Um exemplo concreto desses desafios é apresentado por Norris ao discutir os sistemas de reconhecimento facial baseados em IA. Mesmo os mais avançados destes *softwares*[16] operam sob lógicas simplificadas e redutivas, programadas por humanos, resultando em classificações binárias que podem ter implicações significativas para os indivíduos, como o "acesso aceito ou negado; identidade é aceita ou rejeitada; o comportamento é legítimo ou ilegítimo" (NORRIS, 2003; COSTA; NEGRI; DE OLIVEIRA, 2020, p. 93).

Embora alguns argumentem que as tecnologias de IA possibilitam uma vigilância "democrática", estudos como o de Clive Norris revelam padrões preocupantes de viés e

[15] Em tradução livre, espelho unidirecional.

[16] Nesta pesquisa, o conceito de *software* é o descrito no art. 1º da Lei 9.609/98, "Programa de computador é a expressão de um conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte físico de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados" (BRASIL, 1998).

discriminação. Jovens, homens e pessoas negras são frequentemente alvos desproporcionais de vigilância, mesmo na ausência de comportamentos suspeitos ou criminosos. Esta prática, justificada por "suspeitas" vagas, evidencia a perpetuação de preconceitos sociais através da tecnologia (NORRIS, 2003).

A transição para uma vigilância sistêmica, desprovida de julgamentos morais, resulta em uma avaliação unidimensional dos indivíduos. Como observa Clive Norris, estes sistemas não discernem entre bom ou mau, honesto ou desonesto, pobre ou rico, simplesmente verificam a elegibilidade de acesso a determinados espaços, bens e serviços. Esta abordagem algorítmica à classificação social levanta questões significativas sobre equidade e justiça (NORRIS, 2003).

Neste ponto, cumpre destacar que o desenvolvimento tecnológico se encontra intrinsecamente vinculado aos propósitos e objetivos estabelecidos por seus desenvolvedores e proprietários, atuando como um amplificador das capacidades humanas. Esta relação entre tecnologia e poder econômico manifesta-se de maneira particularmente expressiva no contexto das sociedades capitalistas contemporâneas (POLI; VIEGAS; XAVIER, 2024).

O direcionamento dos investimentos em inovações tecnológicas é substancialmente influenciado pelos detentores de capital, que exercem papel decisivo na determinação das prioridades de desenvolvimento e implementação dessas tecnologias. Esta dinâmica evidencia uma estrutura de poder onde o controle sobre os recursos financeiros traduz-se em capacidade de influência sobre as trajetórias tecnológicas e, consequentemente, sobre as transformações sociais dela decorrentes. Exemplificadamente, são as recomendações de “obras literárias de autores brancos e europeus em detrimento das obras regionais, nos sites de venda de livros, sugerindo um direcionamento automático e inconsciente de preferências culturais” (POLI; VIEGAS; XAVIER, 2024, p. 10).

O quadro da mão de obra disponível para a execução de trabalhos neste setor, conforme as estatísticas recentes demonstram um panorama preocupante quanto à diversidade. Em âmbito global, apenas 5% (cinco porcento) dos profissionais de tecnologia se identificam como mulheres, enquanto no Brasil, dados de 2022 apontam que um percentual de 15% (quinze por cento) como do sexo feminino. Estes números refletem não apenas a autoconcepção dos indivíduos no contexto social, mas também as estruturas estabelecidas nas comunidades de pesquisa e desenvolvimento tecnológico (NALIN, 2024).

O contexto é agravado pela conjunção de fatores sociais e econômicos. A formação profissional na área tecnológica, caracterizada por seu alto custo e acesso restrito, contribui para a perpetuação desta hegemonia demográfica. Simultaneamente, observa-se uma tendência preocupante entre os jovens desenvolvedores, que, motivados por expressivas remunerações e

demonstrando limitada consciência política, frequentemente negligenciam as implicações sociais de suas criações tecnológicas (POLI; VIEGAS; XAVIER, 2024; BRANDÃO; CARBONERA; FERREIRA, 2021).

Este é um retrato que revela uma significativa disparidade “demográfica entre os profissionais da tecnologia, majoritariamente de homens brancos pertencentes às classes socioeconômicas média e alta”. Esta configuração evidencia uma expressiva lacuna na representatividade e no acesso a oportunidades para grupos historicamente marginalizados no setor tecnológico (POLI; VIEGAS; XAVIER, 2024, p. 10).

O que influencia no caráter discricionário destes sistemas, como apontado por Clive Norris resulta em um monitoramento desigual entre diferentes comunidades. Algumas enfrentam uma vigilância punitiva intensiva, enquanto outras experimentam uma abordagem mais "favorável". Este fenômeno é exemplificado pelo uso de câmeras de reconhecimento facial com IA, que “não são instalados para identificar um furto, mas para identificar um indivíduo previamente classificado como praticante de tal delito”. Tais práticas não apenas perpetuam vieses existentes, mas também criam o que especialistas chamam de "falsos positivos", exacerbando discriminações sistêmicas (NORRIS, 2003; COSTA; DE OLIVEIRA; NEGRI, 2000, p.93; BIONI; LUCIANO, 2019).

O impacto destas tecnologias de coleta e processamento de dados vai além do controle comportamental, afetando profundamente a construção da identidade individual. Ramon Silva Costa, Sergio Marcos Carvalho Negri e Samuel Rodrigues De Oliveira destacam como os indivíduos tendem a moldar-se para satisfazer os algoritmos, um fenômeno que impacta na formação da autenticidade e da liberdade pessoal, ou seja, “corpos anônimos podem ser transformados em sujeitos digitais, identificados e relacionados às suas personas digitais que residem em bases de dados eletrônicos” o que ocorre frequentemente sem o consentimento ou controle do indivíduo, evidenciando potenciais violações à privacidade (COSTA; DE OLIVEIRA; NEGRI, 2000; NORRIS, 2003, p.278).

Paradoxalmente, uma parte significativa da sociedade apoia a adoção destes dispositivos de vigilância, atraída pela promessa de segurança e suposta neutralidade. No entanto, mesmo os apoiadores se tornam ‘assujeitados’, submetendo-se a “invasões constantes em sua esfera de intimidade acabam por desapropriá-los de seu espaço de construção de identidade e, consequentemente, do valor dignidade que lhe é devido” (COSTA; NEGRI; DE OLIVEIRA, 2020; BAIÃO; GONÇALVES, 2014).

Neste contexto, Rodotà sugere que a privacidade pode se manifestar como uma necessidade de anonimato, fundamental ao desenvolvimento da personalidade e a plena

realização da liberdade existencial. Esta perspectiva ressalta a importância de proteger não apenas os dados pessoais, mas também o direito de construir e manter uma identidade autêntica e autônoma no espaço digital (RODOTÀ, 2008).

A transição para uma era de psicopolítica digital, como proposto por Han, implica em desafios significativos para a autonomia individual e a privacidade. Nelson Rosenvald e Felipe Braga Netto analisam que a linha entre o mercado de vigilância em estados democráticos e o estado de vigilância digital em regimes autoritários torna-se cada vez mais tênue, com práticas de empresas como Google se assemelhando, em certos aspectos, às de serviços de inteligência estatais, como a China (NETTO, ROSENVALD, 2024).

Em sua obra, Yuval Noah Harari contribui para este debate ao argumentar que a crescente autoridade dos algoritmos sobre diversos aspectos da vida humana está transformando fundamentalmente nossa percepção do mundo e de nós mesmos. Segundo o historiador, à medida que delegamos cada vez mais decisões a sistemas algorítmicos, nossa compreensão da realidade se afasta da noção de indivíduos autônomos fazendo escolhas conscientes, aproximando-se de uma visão do universo como um fluxo contínuo de dados a ser processado e analisado. “Quando a autoridade passa de humanos para algoritmos, não podemos mais ver o mundo como o campo de ação de indivíduos autônomos esforçando-se por fazer as escolhas certas. Em vez disso vamos perceber o universo inteiro como um fluxo de dados” (HARARI, 2018, p.83).

Esta evolução tecnológica e social tem implicações profundas que transcendem a esfera meramente econômica.

Como argumenta Ana Frazão, o capitalismo de dados emergente afeta não apenas as estruturas de mercado, mas também as dimensões políticas, sociais e existenciais da vida cidadã. Os riscos associados a este modelo de capitalismo tornam-se cada vez mais evidentes e graves à medida que avança a integração entre o desenvolvimento tecnológico e a exploração comercial de dados pessoais (FRAZÃO, 2019, p. 34).

Neste contexto, Lawrence Lessig oferece uma contribuição ao posicionar a tecnologia como um regulador de comportamentos, equiparando-a a outras formas tradicionais de controle social. Segundo Lessig, a tecnologia opera ao lado do poder hierárquico das leis, do controle baseado na competição de mercado e das normas sociais comunitárias. Esta visão destaca o papel fundamental que os sistemas tecnológicos desempenham na moldagem das interações sociais e na definição dos limites do comportamento individual e coletivo na era digital (LESSIG, 1999).

A aparente imparcialidade e apoliticidade atribuídas à tecnologia mascaram, muitas vezes, complexas estruturas de poder e tomada de decisão. Surgem, então, os debates sobre a natureza e a legitimidade dessas tecnologias: Como podemos exigir transparência e compreensão quando decisões significativas - como a negação de crédito ou a rejeição em processos seletivos - são tomadas por algoritmos opacos? Como questionar ou contestar decisões baseadas em processos que não compreendemos plenamente? E, talvez mais importante, como podemos mitigar ou eliminar o potencial de decisões arbitrárias e preconceituosas em uma sociedade que aspira à inclusão e à equidade?

Estas indagações não são meramente retóricas, mas refletem preocupações reais e urgentes sobre a governança algorítmica e seu impacto na autonomia individual e na justiça social, nos conduzem naturalmente a uma reavaliação fundamental do conceito de privacidade na era digital.

Na sociedade digital, o tratamento[17] de dados pessoais abrange uma dimensão expansiva, permeando e ressignificando as realidades sociais e a vida cotidiana dos indivíduos. Bruno Bioni argumenta que a proteção aos dados pessoais transcende a mera salvaguarda da privacidade, constituindo-se como tutela da "própria dimensão relacional da pessoa humana". Esta autorização permite que os dados pessoais sejam fonte de diversas liberdades individuais que extrapolam a dicotomia tradicional entre esfera pública e privada (BIONI, 2019; p.99).

Ana Frazão enfatiza a importância de um sistema eficiente de proteção de dados para a manutenção do livre-arbítrio e da democracia, especialmente diante das diversas formas de manipulação possibilitadas pelo uso indevido de dados pessoais. Esta é uma preocupação compartilhada por diversos autores, como Rodotà e Clive Norris, que chamam atenção para “as informações utilizadas são, de fato, sempre parciais e incompletas, mesmo quando se recorre a uma multiplicidade de bancos de dados”. Esta perspectiva reforça a necessidade de normas protetivas que consagrem o princípio da autodeterminação informativa, garantindo aos indivíduos o poder de controlar a circulação de suas próprias informações (FRAZÃO, 2021; NORRIS, 2003; RODOTÀ, 2008, p.115).

O advento e a rápida evolução dos mecanismos de IA, aliados à crescente disponibilidade de informações, deixaram marcas profundas na regulação da proteção de dados pessoais (DONEDA *et al*., 2018).

[17] Este trabalho adota o conceito de tratamento de dados previsto na LGPD, qual seja, tratamento de dados é 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 (art. 5º, X, Lei nº 13.709/18) (BRASIL, 2018).

A concepção tradicional de privacidade, centrada na dicotomia entre público e privado, mostra-se cada vez mais inadequada diante das complexidades do ambiente digital contemporâneo. Estas questões conduzem naturalmente a uma reflexão mais profunda sobre o conceito de privacidade na era digital. No próximo capítulo, 'a evolução do conceito de privacidade na era digital: da proteção massiva à autodeterminação informativa', explorará como a noção tradicional de privacidade está sendo desafiada e redefinida no contexto do capitalismo de vigilância. Analisará as mudanças fundamentais na forma como entender e proteger a privacidade, bem como as novas abordagens legais e éticas necessárias para salvaguardar os direitos individuais em um mundo cada vez mais digitalizado.

À medida que avança, convida-se o leitor a considerar como estas transformações tecnológicas e sociais estão redefinindo não apenas a relação com a informação pessoal, mas também os próprios fundamentos de nossa autonomia e identidade no século XXI. O próximo capítulo oferecerá *insights* sobre como navegar neste novo paradigma, equilibrando os benefícios da inovação tecnológica com a proteção essencial de nossos direitos fundamentais à privacidade e autodeterminação.

3 A EVOLUÇÃO DO CONCEITO DE PRIVACIDADE NA ERA DIGITAL: DA PROTEÇÃO PASSIVA À AUTODETERMINAÇÃO INFORMATIVA

A evolução do conceito de privacidade representa um dos mais significativos desafios jurídicos e sociais da era digital, transcendendo a tradicional compreensão de um direito meramente individual para se configurar como um complexo sistema de proteção de dados e autonomia informativa. Diante das transformações tecnológicas contemporâneas, especialmente com o advento das TICs[18], a privacidade deixa de ser um conceito estático baseado na dicotomia público-privado e se transmuta em um direito fundamental dinâmico, que exige não apenas a abstenção de interferências, mas uma proteção proativa capaz de garantir o controle individual sobre informações pessoais. Este capítulo analisa criticamente essa transição conceitual, explorando como o direito à privacidade se ressignifica no contexto do *big data*, das decisões algorítmicas e das práticas de perfilamento digital, evidenciando a necessidade de uma abordagem multidimensional que proteja não apenas indivíduos, mas também grupos e coletividades contra potenciais danos informacionais.

A evolução histórica do conceito de privacidade reflete as profundas transformações sociais e tecnológicas que caracterizam a era digital. Tradicionalmente, a noção de privacidade era compreendida através da dicotomia entre o público e o privado, como elucida Danilo Doneda. Esta concepção clássica estabelecia uma distinção clara entre as atividades exercidas no domínio público e aquelas resguardadas na esfera privada, com as estruturas arquitetônicas servindo como barreiras físicas contra o escrutínio público. Portanto, “há uma seleção entre as informações que podem ser partilhadas publicamente e aquelas que devem ser mantidas no sigilo privado”. Mesmo que as informações intimas fossem “compartilhadas com maior ou menor número de pessoas, restringem-se ao controle dos indivíduos e ao seu interesse em mantê-las distantes do público em geral” (DONEDA, 2021; COSTA; NEGRI; DE OLIVEIRA, 2020, p. 89).

Verifica-se que o conceito exposto se solidificava na visão clássica do direito à privacidade, cuja a base são posições como “*the right be left alone*[19]”, formulado por Warren e

[18] Tecnologias da Informação e Comunicação (TICs) podem ser definidas como o conjunto total de tecnologias que permitem a produção, o acesso e a propagação de informações, assim como tecnologias que permitem a comunicação entre pessoas. Com a evolução tecnológica, surgiram novas tecnologias, que se propagaram pelo mundo como formas de difusão de conhecimento e facilitaram a comunicação entre as pessoas, independentemente de distâncias geográficas (RODRIGUES *et al*., 2014).

[19] "The right to be left alone" é uma expressão que se refere ao direito fundamental à privacidade. Foi popularizada pelo jurista americano Louis Brandeis em um artigo de 1890 co-escrito com Samuel Warren, intitulado "The Right to Privacy". Eles definiram esse direito como a mais abrangente das liberdades e a mais valorizada pelos

Brandeis[20], que enfatizava primordialmente o aspecto negativo da privacidade. Tal perspectiva focava na proteção contra intrusões indesejadas na esfera pessoal do indivíduo, estabelecendo um paradigma de privacidade centrado na exclusão e no sigilo (BRANDEIS; WARREN, 2024).

As relações assumem formas inéditas, a privacidade emerge como um direito fundamental particularmente vulnerável. Helen Nissenbaum destaca que os novos riscos à privacidade no ciberespaço exigem intervenções estruturais preventivas, reconhecendo a natureza proativa necessária para a proteção de dados na era digital. Enquanto para José Faleiros Junior e Filipe Medon, baseando-se nos trabalhos de William Staples, alertam para "os riscos de que a violação a práticas como a perfilização pode causar ao direito fundamental à privacidade". Esta observação ressalta a necessidade de uma abordagem mais sofisticada e abrangente para a proteção da privacidade em um contexto de coleta e análise massiva de dados (NISSENBAUM, 2010; FALEIROS JUNIOR; MEDON, 2021; STAPLES, 2007, p.93).

Nesta linha de raciocínio, Stefano Rodotà foi pioneiro ao propor uma expansão do conceito de privacidade para abarcar não apenas o direito de ser deixado só, mas também o direito de controlar ativamente as informações pessoais e construir a própria esfera privada. Para o autor, o conceito precisava de um elastecimento para abranger não só o direito de ser deixado só, mas também o direito de controlar as informações pessoais e de construir a esfera privada. Portanto, o direito evoluiria para incluir a proteção de dados pessoais, alcançando, "não só o poder de exclusão, ou seja, de impedimento de interferências alheias, mas também compreende a centralidade do controle do indivíduo sobre suas informações pessoais". Esta evolução conceitual reflete a transição de uma tríade "pessoa-informação-sigilo" para um modelo quadripartite que inclui "pessoa-informação-circulação-controle" (RODOTÀ, 2013; COSTA; NEGRI; DE OLIVEIRA, 2020, p. 89).

As transformações tecnológicas influenciam na transmutação do conceito de privacidade, que conforme o mercado altera, o conceito também reformula, como "o direito a controlar o uso que os outros façam das informações que me digam respeito", e com o aprimoramento das ferramentas, passou-se para "um outro tipo de definição, segundo o qual a

cidadãos, essencialmente afirmando que os indivíduos têm o direito de viver sem interferências ou intrusões não desejadas por parte do governo, de outras pessoas ou de entidades privadas.

[20] O ensaio "O Direito à Privacidade" é considerado uma obra seminal que inaugurou os debates sobre privacidade nos Estados Unidos. Esta publicação enfatiza o papel crucial da privacidade como elemento fundamental da autonomia e dignidade do ser humano. Os autores argumentam que qualquer violação da privacidade constitui uma afronta aos direitos individuais, evidenciando uma clara intenção de proteger a personalidade humana em sua integralidade. Esta abordagem estabeleceu as bases para o reconhecimento da privacidade como um direito essencial, influenciando significativamente o pensamento jurídico e social subsequente sobre o tema. A obra destaca-se por sua visão pioneira em vincular a privacidade diretamente à noção de direitos humanos fundamentais (BRANDEIS; WARREN, 2024).

privacidade consubstancia-se no “direito do indivíduo de escolher aquilo que está disposto a revelar aos outros”. Esta mudança reflete uma compreensão mais ampla e ativa da privacidade na era digital. Como observa Han, há "uma falta total de distância, na qual a intimidade é exposta publicamente e o privado se torna público". Esta realidade implica que as interferências não se limitam mais apenas ao direito à privacidade tradicional, mas se estendem também à proteção de dados em um sentido mais amplo (RODOTÀ, 2013, p. 74; RODOTÀ, 2018ª, p.12).

A evolução do conceito de privacidade é notável. O que antes era entendido simplesmente como "o direito de ser deixado só" agora se expande para abranger a proteção abrangente das escolhas de vida contra formas de controle político e estigmatização social. Esta expansão visa salvaguardar a liberdade nas escolhas existenciais e políticas dos indivíduos.

Neste novo contexto, emerge o conceito de autodeterminação informativa como uma evolução necessária do direito à privacidade. Bruno Bioni e Laura Schertel Mendes argumentam que a proteção de dados pessoais deve ser reconhecida como um direito fundamental autônomo, transcendendo a mera extensão do direito à privacidade. Esta perspectiva reconhece a autodeterminação informativa, representa uma mudança paradigmática, transformando a privacidade de um direito passivo em um direito ativo. Esta nova concepção demanda não apenas a abstenção de interferências, mas também ações afirmativas por parte do Estado e de entidades privadas para garantir a proteção efetiva dos dados pessoais (BIONI, 2019; MENDES, 2014).

Stefano Rodotà oferece uma definição abrangente deste direito, caracterizando-o como a capacidade do indivíduo de manter controle sobre suas próprias informações e determinar a construção de sua esfera privada. No entanto, o autor alerta para a ameaça significativa representada pela criação de perfis detalhados baseados em dados pessoais, uma prática cada vez mais comum na era do *big data* (RODOTÀ, 2008).

O conceito de autodeterminação informativa, fundamental para a compreensão moderna da proteção de dados, tem suas raízes na decisão histórica da Corte Constitucional Alemã em 1983[21]. Esse reconhecimento é uma via de mão dupla: proteger os indivíduos em relação aos

[21] O conceito de autodeterminação informativa tem sua gênese em uma decisão histórica da Corte Constitucional alemã (Bundesverfassungsgericht) em 15 de dezembro de 1983. O caso em questão abordava a constitucionalidade da Lei do Recenseamento de População, Profissão, Moradia e Trabalho, promulgada em 25 de março do mesmo ano. Neste julgamento emblemático, a Corte declarou parcialmente inconstitucional a referida lei. O fundamento desta decisão baseou-se na premissa de que certos dispositivos da lei comprometiam o direito fundamental dos cidadãos ao livre desenvolvimento de sua personalidade. Argumentou-se que estes dispositivos privavam os indivíduos da capacidade de gerenciar o fluxo de suas informações pessoais coletadas pelo Estado. A importância deste julgamento é destacada por Laura Schertel Mendes, que observa que a decisão da Corte Constitucional estabeleceu um marco na teoria da proteção de dados pessoais. Ao formular o direito à autodeterminação da informação, a Corte não apenas reconheceu um direito subjetivo fundamental, mas também posicionou o indivíduo como figura central no processo de tratamento de seus próprios dados. Este entendimento

riscos à sua personalidade em razão da coleta, tratamento, uso e circulação de dados, em outro lado, visa garantir que tenha o controle sobre o fluxo de seus dados pessoais (MENDES, 2014).

No Brasil, a importância deste direito foi evidenciada no julgamento da ADI 6.387/DF e na ADI 6389/DF pelo Supremo Tribunal Federal. Neste caso, o tribunal examinou a constitucionalidade da Medida Provisória 954/2020[22], que autorizava o compartilhamento de dados pessoais de clientes de operadoras de telefonia com o IBGE para fins de pesquisas estatísticas durante a pandemia de COVID-19. A decisão do STF reafirmou a importância da proteção de dados pessoais como um direito fundamental, estabelecendo limites claros para o uso e compartilhamento de informações pessoais, mesmo em situações de emergência pública.

No acordão da ADI 6389/DF em uma análise minuciosa conduzida pela Ministra Relatora Rosa Weber evidenciou os riscos potenciais associados ao compartilhamento indiscriminado de dados pessoais, como nomes, números telefônicos e endereços. Em seu voto, a Ministra destacou a evolução tecnológica que transformou radicalmente o cenário de utilização de dados pessoais:

> Certamente há quem ainda se lembre de que há poucas décadas, antes da ubiquidade da telefonia móvel, era comum a edição de listas telefônicas impressas contendo nomes, telefones e endereços dos assinantes residenciais e comerciais dos serviços de telefonia em uma dada localidade. Além de ser facultado aos usuários dos serviços de telefonia optarem pela exclusão dos próprios dados dessas listas, é crucial ter presente que o que podia ser feitos a partir da publicização de tais dados pessoais não se compara ao que pode ser feito no patamar tecnológico atual, em que poderosas tecnologias de processamento, cruzamento e filtragem de dados permitem a formação de perfis individuais extremamente detalhados.(BRASIL, 2020, p. 16)

Esta reflexão da Ministra Weber sublinha a transformação radical no potencial de uso e abuso de dados pessoais na era digital. O que antes era uma simples lista impressa tornou-se, com o advento de tecnologias avançadas de processamento de dados, uma fonte potencial para a criação de perfis detalhados e invasivos.

A decisão do STF, ao suspender a eficácia da MP 954/2020, estabeleceu um precedente crucial para a proteção da privacidade e da autodeterminação informativa no Brasil. Este julgamento evidencia a necessidade de um equilíbrio cuidadoso entre as necessidades de coleta

influenciou significativamente as subsequentes legislações nacionais e europeias sobre o tema (MENDES, 2014).

[22] A Medida Provisória (MP) nº 954/2020 foi uma norma jurídica que autorizava a divulgação de dados pessoais de consumidores de telefonia fixa e móvel ao IBGE. A MP 954/2020 foi editada pelo Presidente da República em situações de urgência e relevância, como previsto na Constituição. No entanto, a norma foi questionada por violar o direito à privacidade (BRASIL, 2020).

de dados para fins públicos e a preservação dos direitos individuais à privacidade e ao controle sobre informações pessoais.

Um aspecto particularmente relevante desta decisão é o reconhecimento da opacidade e da natureza dinâmica das técnicas modernas de criação de perfis. Estes processos, muitas vezes realizados sem o conhecimento ou consentimento explícito dos indivíduos, criam uma lacuna significativa entre o propósito original da coleta de dados e suas aplicações subsequentes. Esta situação levanta questões fundamentais sobre a eficácia prática do direito à autodeterminação informativa[23] em um contexto tecnológico em rápida evolução.

Frente a estes desafios, autores como Michael Froomkin argumentam pela urgência na adoção de medidas que limitem práticas invasivas, alertando para o risco de uma sociedade sem privacidade, metaforicamente descrita como um *goldfish bowl*[24]*,* o que representa "metonímia utilizada pelo autor para se referir ao aquário transparente no qual peixes-dourados são usualmente expostos, sem qualquer privacidade" (FROOMKIN, 2000; FALEIROS, MENDON, 2021, p. 962)

Adicionalmente, Nadezhda Purtova introduz o conceito de "*information-induced-harms*" (danos causados pela informação), definidos como qualquer consequência negativa, seja pública ou individual, resultante do processamento de informações. Esta perspectiva amplia consideravelmente o entendimento dos potenciais impactos negativos do uso indevido de dados pessoais (PURTOVA, 2018).

Todo este contexto, além de ampliar o campo de proteção da privacidade, notou-se a importância de prever como um direito fundamental no texto constitucional. Encabeçado por estudiosos do direito como Danilo Doneda, Laura Schertel Mendes e Caitlin Mulholland que defenderam veementemente a inclusão deste direito no rol de garantias fundamentais dos indivíduos, argumentando que esta proteção é essencial para salvaguardar a dignidade e a autonomia pessoal na era digital. Em favor do reconhecimento da proteção de dados como direito fundamental baseia-se em uma interpretação holística de diversos dispositivos

[23]Uma situação que exemplifica os obstáculos enfrentados pela autodeterminação informativa ocorre frequentemente no uso de aplicativos e plataformas digitais. Nestas, os usuários são solicitados a consentir com o processamento de seus dados pessoais. Contudo, a escolha apresentada é muitas vezes restrita: ou o usuário concorda com a coleta completa dos dados requeridos, ou enfrenta limitações significativas no acesso aos serviços oferecidos. Este cenário cria uma conjuntura onde o usuário se vê praticamente forçado a ceder o controle sobre suas informações pessoais para poder utilizar um determinado serviço. Tal prática suscita dúvidas quanto à autenticidade da liberdade de escolha do usuário e à real validade do consentimento obtido nestas condições. A abordagem binária em relação à autorização para o tratamento de dados pessoais coloca em questão a verdadeira autonomia do indivíduo sobre suas informações. Consequentemente, esta prática pode comprometer seriamente o princípio fundamental da autodeterminação informativa, ao reduzir drasticamente as opções disponíveis ao usuário no que diz respeito ao controle de seus próprios dados.

[24] Em tradução livre, goldfish bowl significa aquário redondo.

constitucionais. O artigo 5º, inciso X[25], da Constituição Federal, que garante a inviolabilidade da intimidade e da vida privada, o instituto do *habeas data*[26], e o princípio da dignidade da pessoa humana[27] formam a base desta argumentação. Laura Schertel Mendes enfatiza a necessidade de proteção frente às ameaças aos direitos da personalidade na era digital, enquanto Danilo Doneda ressalta a relevância dos princípios constitucionais da igualdade e liberdade neste contexto (DONEDA, 2011; MULHOLLAND, 2018; MENDES, 2014).

Diante deste debate, um marco significativo foi a aprovação da PEC 17/2019[28], que resultou na Emenda Constitucional nº 115 de 2022. Esta emenda elevou explicitamente a proteção de dados pessoais ao status de direito fundamental, incluindo-a no art. 5º, inciso LXXIX, da CF[29]. Além disso, acrescentou o inciso XXX ao artigo 22[30] e o inciso XXVI ao artigo 21[31], estabelecendo a competência exclusiva da União para legislar sobre esta matéria.

Não se pode esquecer que o princípio da autodeterminação informativa, foi consagrado na LGPD, representando um marco fundamental na legislação brasileira de proteção de dados pessoais. Ao incorporar este conceito em sua estrutura normativa, especificamente no artigo 2º, inciso II[32], a LGPD eleva a autodeterminação informativa de uma noção doutrinária a um princípio legal concreto, reafirmando o compromisso do ordenamento jurídico brasileiro com o empoderamento dos indivíduos no controle de suas informações pessoais.

No entanto, a implementação efetiva deste princípio enfrenta desafios consideráveis no ambiente digital contemporâneo. A prática comum de plataformas e aplicativos de oferecer escolhas limitadas aos usuários quanto ao uso de seus dados pessoais frequentemente resulta

---

[25] Art. 5º, X — "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" (BRASIL, 1988).

[26] O habeas data é um remédio constitucional que garante o direito de acesso a informações e retificação de dados. A lei também prevê a possibilidade de complementação de informações, não prevista na Constituição. O habeas data pode ser impetrado por qualquer cidadão brasileiro, mas é necessário o auxílio de um advogado ou defensor público. A ação é gratuita e tem prioridade sobre outros atos judiciais, exceto o habeas corpus e o mandado de segurança. O requerimento do habeas data deve ser apresentado ao órgão ou entidade que possui o registro ou banco de dados, que tem 48 horas para responder. A decisão é comunicada ao requerente em até 24 horas. Para que o habeas data seja impetrado, é necessária a prova de que a autoridade administrativa recusou as informações. Caso não haja essa prova, a ação é extinta por falta de interesse processual. Previsto no art. 5º, LXXII da CF/88 e regulamentado na Lei nº 9.507/97.

[27] Art. 1º, III, da Constituição Federal.

[28] Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

[29] Art. 5º. [...]. LXXIX – "e assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais". (BRASIL, 1988).

[30] Art. 22. [...]. "Compete privativamente à União legislar sobre: [...] XXX - proteção e tratamento de dados pessoais." (BRASIL, 1988)

[31] Art. 21. [...]. "Compete à União: [...] XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei". (BRASIL, 1988)

[32] Art. 2º "A disciplina da proteção de dados pessoais tem como fundamentos: [...] II - a autodeterminação informativa." (BRASIL, 1988)

em um consentimento que pode ser questionado quanto à sua autenticidade e validade. Bioni argumenta que este cenário de "tudo ou nada" em relação ao consentimento para o tratamento de dados pessoais coloca em xeque a verdadeira autonomia do indivíduo sobre suas informações (BIONI, 2019).

Portanto, em uma análise contemporânea das questões de privacidade e proteção de dados, é essencial adotar uma perspectiva coletiva. Esta abordagem foca nos potenciais riscos associados ao uso discriminatório e inadequado do tratamento de dados que afetam grupos inteiros de indivíduos categorizados em perfis similares. Conceitos como privacidade de grupo (*group privacy*) e proteção coletiva de dados pessoais (*collective data protection*) emergem como fundamentais nesta discussão (MANTELERO, 2016).

No cenário atual de análise de dados em larga escala, o foco não está necessariamente no perfil de um único usuário, mas sim nos agrupamentos (*clusters*) ormados a partir da coleta e análise de dados de milhões de indivíduos. As políticas e decisões são frequentemente baseadas em perfis e padrões coletivos, afetando grupos ou categorias inteiras de pessoas, seja positiva ou negativamente. Como afirma Stefano Rodotá trata-se de uma “tutela global das escolhas da vida contra qualquer forma de controle político e de estigmatização social”. Esta abordagem enfatiza a importância de compreender como determinados grupos são impactados, se podem agir com autonomia e se são tratados com dignidade (RODOTÁ, 2008, p.129).

Esta abordagem coletiva reconhece que, embora indivíduos específicos possam ser afetados por certos usos de dados, o impacto mais significativo e abrangente ocorre no nível de grupos e categorias sociais. Consequentemente, as estratégias de proteção e as políticas regulatórias devem ser adaptadas para abordar esses desafios em uma escala mais ampla e coletiva. Esta mudança de perspectiva reflete a realidade da era da *big data*, onde os efeitos das práticas de análise de dados transcendem o nível individual, tornando-se uma questão de impacto coletivo e social.

Assim, reflete a necessidade de observar a natureza difusa do dano causado pelo tratamento inadequado dos dados, um aspecto que não foi plenamente reconhecido anteriormente, mas que pode ser vislumbrada na LGPD ao adota uma estrutura dual, combinando a proteção individual dos titulares de dados com a salvaguarda de direitos difusos (MENDES, 2014).

A legislação protetiva dos dados incorpora uma dimensão coletiva de proteção, ao prever a possibilidade de defesa coletiva dos interesses dos titulares de dados em juízo (art.

22[33]) e perante organismos de defesa do consumidor (art. 18, §8º[34]), isso inclui como "Procons, Defensoria Pública, ONGs e Ministérios Públicos – o que é chamado de Sistema Nacional de Defesa do Consumidor". Esta abordagem reflete o reconhecimento da natureza difusa dos danos potenciais resultantes do tratamento inadequado de dados (ZANATTA, 2020, p. 346-347).

A legislação estabelece uma forte conexão com o CDC e com o sistema de tutela coletiva brasileiro. Isso permite que a proteção de dados pessoais seja realizada não apenas individualmente, mas também de forma coletiva, através de diversos mecanismos legais (ZANATTA, 2019).

Esta perspectiva coletiva da privacidade e proteção de dados exige uma avaliação do impacto do tratamento de dados na comunidade como um todo, possibilitando reparações coletivas quando necessário (ZANATTA, 2019).

Embora a tutela coletiva tenha um forte componente processual, o aspecto mais relevante para esta discussão é o reconhecimento da dimensão coletiva da proteção de dados e da privacidade. Isso tem implicações significativas para a implementação de mecanismos de salvaguarda em casos de uso de dados pessoais em decisões automatizadas baseadas em algoritmos de aprendizado de máquina.

Este reconhecimento fornece base para a implementação de medidas que visam assegurar uma "*accountability*[35] algorítmica binária". Este conceito engloba tanto uma dimensão de direitos individuais quanto de interesses coletivos, buscando justificar e apresentar diferentes abordagens para a prestação de contas, especialmente no que diz respeito ao direito à explicação de decisões algorítmicas (KAMINSKI, 2019b).

A complexidade deste cenário se torna ainda mais evidente quando consideramos as práticas de perfilamento digital, tema que será explorado em profundidade no próximo capítulo. O perfilamento, como uma manifestação concreta dos desafios à autodeterminação informativa, representa um ponto crítico onde os princípios legais enfrentam as realidades práticas do processamento de dados em larga escala. A análise das técnicas de perfilamento e suas implicações para a privacidade e autonomia individual oferecerá uma perspectiva crucial sobre como os princípios da LGPD se traduzem em proteções efetivas no mundo digital.

---

[33] Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva (BRASIL, 1988).

[34] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: [...] § 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor (BRASIL, 1988).

[35] O conceito de accountability será apresentado e destrinchado no tópico 5.4.4. Responsabilidade civil: entre a prevenção e a explicabilidade.

Ao adentrar o próximo capítulo, este trabalho irá explorar as práticas de perfilamento digital interagem com o princípio da autodeterminação informativa, examinando os desafios específicos que emergem quando algoritmos complexos são empregados para categorizar e prever comportamentos individuais. Esta análise não apenas aprofundará a compreensão dos desafios contemporâneos à privacidade, mas também iluminará os caminhos possíveis para a efetiva proteção dos direitos individuais na era da informação.

4 PERFILAMENTO DIGITAL: IMPLICAÇÕES ÉTICAS E JURÍDICAS DA ANÁLISE PREDITIVA DE DADOS PESSOAIS

A perfilização, também conhecida como *profiling* ou perfilamento automatizado, é uma prática cada vez mais prevalente na era digital. Definida como o "registro sistemático, proposital e classificatório de dados relacionados aos indivíduos", esta técnica transcende a simples categorização. Segundo José Faleiros e Filipe Medon, trata-se da "utilização de dados pessoais para categorizar preferências e interesses, usualmente, com o intuito de obtenção de alguma vantagem" (TUMELERO, 2021, p. 67; FALEIROS; MEDON, 2021, p.949).

Seu objetivo principal vai além da mera identificação, propondo-se a antecipar padrões futuros de comportamento, tanto de indivíduos quanto de grupos específicos. Nesse sentido, busca prever não apenas as ações prováveis de um indivíduo, mas também as trajetórias potenciais de grupos inteiros que compartilham características similares, como observa Danilo Doneda (DONEDA, 2021).

O processo de perfilamento, originalmente enraizado nas Ciências Criminais para "reconstruir determinado crime a partir da análise detalhada da cena do crime ou do perfil do suposto criminoso", expandiu-se significativamente em sua aplicação contemporânea. Através da análise de dados históricos e atuais, esta abordagem busca delinear o possível curso de ação ou "destino" de uma pessoa ou conjunto de pessoas que se enquadram em determinado perfil (FALEIROS; MEDON, 2021, p. 949).

A técnica permite a criação de modelos preditivos aplicáveis em diversos contextos, desde marketing personalizado até avaliações de risco em diferentes setores. Ao examinar padrões comportamentais, o perfilamento não se limita mais à investigação criminal, mas se tornou uma ferramenta versátil para compreender e antecipar comportamentos em múltiplas áreas.

No contexto ciberespaço[36], se caracteriza pela reunião e análise algorítmica de dados pessoais em larga escala, resultando no que é conhecido como *big data*. Esta prática é

[36] O ciberespaço é um espaço virtual que reúne pessoas e empresas interconectados por meio de computadores. Ele remete ao espaço das redes digitais, que é o resultado das interconexões de redes de computadores. No ciberespaço, os seres humanos conectam-se às tecnologias com base na internet. Esse conceito foi idealizado pelo escritor norte-americano William Gibson em sua obra "Neuromancer", publicada em 1984. Gibson descreveu o ciberespaço como um espaço virtual constituído por computadores e usuários interligados numa rede mundial. Além da internet, o ciberespaço inclui diversos elementos, como cabos, computadores, informações trocadas, dados e as pessoas que operam esses sistemas. Essa vasta e complexa estrutura compreende a Internet, uma rede mundial de computadores interconectados que torna viável a comunicação online numa escala global. Programação e linguagens de programação também são elementos usados no desenvolvimento de software e algoritmos que constroem as bases do ciberespaço (SOUSA, 2023).

impulsionada pela crescente capacidade tecnológica de processar vastas quantidades de informações, possibilitando análises e combinações complexas. Impulsionado pela capacidade tecnológica de processar todas as informações, possibilitando as análises, combinações que podem ser feitas (BÜCHI *et al,* 2020).

A sofisticação das técnicas de perfilamento é evidenciada pela diversidade de fontes de dados utilizadas. Além das informações fornecidas voluntariamente pelos usuários (como nome, endereço e dados de cartão de crédito), há um crescente uso de dados coletados passivamente através de como *gadgets*[37] e *wearables*[38], por exemplo, dados de frequência cardíaca ou contagem de passos registrados por um relógio inteligente[39]. Estes dispositivos, que prometem monitorar diversos aspectos da saúde e do bem-estar do usuário, também representam uma fonte rica de dados comportamentais (FALEIROS; MEDON, 2021).

Isso ocorre, por exemplo, quando o usuário preenche formulários ou realiza cadastros, tendo como resultado a otimização "quanto a veiculação de publicidade, robustecida pela utilização de *cookies*[40], a precificação e o estímulo ao consumo". Embora estejam cientes dos serviços que estão utilizando, muitas vezes desconhecem a extensão do monitoramento ao qual estão sujeitos (FALEIROS; MEDON, 2021, p. 949).

Como observam José Faleiros e Felipe Medon, esta técnica permite antecipar "as preferências do consumidor, a ponto de, até mesmo, predizer seu comportamento negocial",

---

[37] *Gadgets* é um termo utilizado para designar dispositivos eletrônicos portáteis, como relógio, celular, carregador sem fio.

[38] *Wearables* são assim denominadas as tecnologias vestíveis ou dispositivos vestíveis, são tecnologias que se apresentam na forma de dispositivos iguais ou similares a peças de roupa ou equipamentos vestíveis, tais como relógios, pulseiras ou até mesmo óculos de realidade virtual.

[39] Também, denominam de objetos inteligentes, são objetos físicos se conectem à internet e troquem dados com outros dispositivos e sistemas.

[40] Os cookies são elementos fundamentais na navegação online moderna. Trata-se de pequenos arquivos de texto criados pelos sites que visitamos e armazenados em nossos dispositivos. Esses arquivos desempenham um papel crucial na personalização da experiência do usuário na internet. Existem dois tipos principais de cookies: os temporários e os permanentes. Os cookies temporários são armazenados na memória RAM do computador e são eliminados assim que o navegador é fechado. Por outro lado, os cookies permanentes são gravados no disco rígido e persistem mesmo após o encerramento da sessão de navegação. A função primordial dos cookies é proporcionar uma navegação mais conveniente e eficiente. Eles permitem que os sites "lembrem" as preferências e informações dos usuários, evitando a necessidade de inserir os mesmos dados repetidamente a cada visita. Isso resulta em uma experiência de navegação mais fluida e personalizada. No entanto, é importante notar que os cookies também levantam questões relacionadas à privacidade online. Eles têm a capacidade de coletar diversas informações sobre o usuário, como o endereço IP, o tipo de navegador e sistema operacional utilizados, horários de acesso, páginas visitadas e até mesmo a origem do acesso (por exemplo, se o usuário chegou ao site através de um link). O endereço IP, em particular, é uma informação sensível, pois pode ser usado para identificar o provedor de internet e, potencialmente, a localização geográfica do usuário. Alguns especialistas em segurança digital comparam o IP a uma "impressão digital", devido à sua capacidade de identificação única. Diante dessas considerações, é crucial que os usuários estejam cientes do funcionamento dos cookies e das implicações para sua privacidade online. Muitos navegadores oferecem opções para gerenciar ou limitar o uso de cookies, permitindo um maior controle sobre as informações compartilhadas durante a navegação na internet (DENSA; DANTAS, 2021; QUEIROZ, 2002, p. 88).

tornando uma característica particularmente relevante do perfilamento é sua capacidade de aumentar o poder contratual do fornecedor. Isso representa um risco significativo, especialmente no que diz respeito ao poder de contratar, potencialmente ampliando as disparidades já existentes nas relações de consumo (FALEIROS; MEDON, 2021, p.951).

Nota-se que o propósito fundamental deste processo é fornecer uma base para tomada de decisões, como observa Hildebrandt, podendo ser executadas de forma totalmente automatizada, sem necessidade de intervenção humana direta. Esta abordagem permite que sistemas computacionais utilizem perfis gerados para fazer escolhas ou recomendações de maneira autônoma, representando uma mudança paradigmática na forma como decisões são tomadas (HILDEBRANT, 2008).

A transferência significativa do processo decisório para algoritmos e sistemas de IA altera fundamentalmente a dinâmica de tomada de decisões em diversos contextos. Os sistemas computacionais não apenas processam informações, mas passam a ter capacidade de fazer escolhas e recomendações de forma independente, superando a necessidade de intervenção humana direta em múltiplas situações.

O processo de construção desses perfis é complexo. Conforme Mireille Hildebrandt explica, o agrupamento é gerado a partir de correlações entre os dados, seja através de eventos, como atributos, conferindo um conjunto de propriedades, ou a partir de características comuns a grupos de pessoas que constituem uma comunidade. Este processo de categorização pode resultar em dois tipos principais de perfis: distributivos, onde as características são compartilhadas por todos os membros de um grupo, e não distributivos, onde apenas alguns integrantes compartilham certas características (HILDEBRANT, 2008).

A categoria de perfis não distributivos merece atenção especial devido às suas implicações jurídicas e sociais potencialmente significativas, pois um indivíduo pode ser associado a um perfil e sofrer consequências mesmo sem possuir todas as características definidoras desse grupo. Esta situação levanta questões importantes sobre justiça e equidade na aplicação de sistemas baseados em perfis (HILDEBRANT, 2008).

Os algoritmos responsáveis pela geração desses perfis frequentemente se baseiam em correlações, sem necessariamente fornecer explicações causais para as categorizações realizadas. Esta falta de transparência tem sido alvo de críticas, levando diversos pesquisadores a argumentar contra o uso de modelos puramente correlacionais em determinados contextos, especialmente aqueles que envolvem decisões com impactos significativos na vida das pessoas (ZARSKY, 2013; SELBST; BAROCAS, 2018).

Um desafio adicional neste campo é o fenômeno das ‘correlações espúrias’, onde eventos altamente correlacionados não possuem relação causal real. Este fenômeno pode levar a conclusões utilizadas em muitos sistemas de IA modernos frequentemente ultrapassa a capacidade humana de compreender plenamente a relevância dos critérios utilizados, criando uma ‘caixa preta’ decisória (HILDEBRANDT, 2008).

O fenômeno da perfilização e análise de dados em larga escala tem sido frequentemente referido como ‘datificação’[41]. Este processo, associado ao desenvolvimento de tecnologias de baixo custo e técnicas inovadoras, tem criado novos modelos de negócios e métodos de tratamento de dados. Empresas de tecnologia como o Google têm sido pioneiras nesta prática. Um exemplo notório ocorreu em março de 2021, quando o Google admitiu que seus veículos do *Street View*[42] inadvertidamente coletaram dados pessoais, incluindo mensagens de e-mail e vídeos transmitidos por redes Wi-Fi privadas (CAMPOS, 2012).

No cenário contemporâneo do *marketing* e análise de consumidores, as tecnologias avançadas de processamento de dados e IA têm revolucionado as estratégias de personalização e direcionamento. Esta evolução tecnológica proporciona às empresas uma capacidade sem precedentes de compreender e influenciar o comportamento do consumidor, baseando-se em uma análise minuciosa de dados detalhados sobre localização, hábitos e padrões de consumo.

As empresas agora podem criar perfis de consumidores altamente detalhados e precisos, permitindo a customização de produtos, serviços e mensagens publicitárias em um nível anteriormente inimaginável. Esta capacidade de *microtargeting*[43] não apenas aumenta a eficácia das campanhas de marketing, mas também promete melhorar a experiência do consumidor através de ofertas mais relevantes e personalizadas.

Questões relacionadas à privacidade, ao consentimento informado e ao potencial de manipulação subliminar do comportamento do consumidor estão no centro do debate ético contemporâneo. A linha tênue entre personalização benéfica e intrusão prejudicial na privacidade individual torna-se cada vez mais difícil de discernir (ZUBOFF, 2018).

O tratamento e a classificação dos dados coletados são realizados com um foco primordial na sua utilidade para atividades econômicas, como destacado por Ana Frazão. Ou

---

[41] Este termo foi conceituado na página 31.

[42] O *Google Street View* é um recurso do *Google Maps* e do *Google Earth* que permite ver imagens panorâmicas de 360° de ruas e outras áreas. O *Street View* é composto por bilhões de imagens que podem ser de origem Google ou de colaboradores (GOOGLE, 2024).

[43] *Microtargeting* é uma técnica criada nos EUA que ajuda os políticos a definirem o seu público de um modo específico e descobrir quem seriam os seus potenciais apoiadores. Com o passar do tempo essa estratégia foi passada para o marketing e podemos concluir que o Microtargeting é uma estratégia para individualizar ao máximo os consumidores, e utiliza-se de uma comunicação focada em grupos específicos, pensando em qualidade e não em quantidade.

seja, é um processo que permite que provedores de serviços alcancem indivíduos de maneira altamente direcionada, seja através de anúncios personalizados, posicionamento estratégico de produtos ou serviços, ou até mesmo por meio de gatilhos mentais específicos. Tais práticas, embora potencialmente benéficas para as empresas e, em alguns casos, para os consumidores, levantam questões sobre autonomia e livre arbítrio no contexto do consumo (FRAZÃO, 2018a).

A programação dos algoritmos utilizados por estes provedores é projetada para extrair e analisar padrões que influenciam as decisões de consumo. Esta análise abrange tanto aspectos objetivos quanto subjetivos do comportamento do consumidor, muitas vezes adentrando áreas sensíveis e potencialmente controversas. Ana Frazão enumera uma série de capacidades alarmantes destes sistemas, que vão desde a avaliação de características pessoais e orientação sexual até a análise de estados emocionais e a previsão de propensões a determinados comportamentos ou condições de saúde:

> (...) avaliar as características, a personalidade, as inclinações e as propensões de uma pessoa, inclusive no que diz respeito à sua orientação sexual; analisar o estado de ânimo ou de atenção de uma pessoa; identificar estados emocionais, pensamentos, intenções e mesmo mentiras; (iv) detectar a capacidade e a habilidade para determinados empregos ou funções; (v) analisar a propensão à criminalidade; (vi) antever sinais de doenças, inclusive depressão, episódios de mania e outros distúrbios, mesmo antes da manifestação de qualquer sintoma (FRAZÃO, 2020, p. 1051).

A habilidade de identificar estados emocionais, pensamentos e até mesmo intenções ocultas dos indivíduos representa uma intrusão significativa na privacidade mental, um conceito que até recentemente permanecia fora do alcance da tecnologia. Além disso, a capacidade de detectar aptidões para empregos específicos ou analisar propensões à criminalidade pode levar a práticas discriminatórias, reforçando preconceitos existentes ou criando novos (O'NEIL, 2021).

Particularmente preocupante é a capacidade de prever condições de saúde, incluindo transtornos mentais, antes mesmo da manifestação de sintomas visíveis. Embora esta capacidade possa ter aplicações benéficas na medicina preventiva, impacta em pontos éticos sobre o direito à privacidade médica e o potencial para discriminação baseada em predisposições genéticas ou comportamentais.

Os dados que compõem os perfis digitais dos indivíduos são provenientes de diversas fontes, abrangendo desde informações fornecidas voluntariamente pelos usuários até dados extraídos através de técnicas sofisticadas de mineração e análise. As técnicas de raspagem de

dados[44], por exemplo, permitem a coleta automatizada de informações disponíveis em plataformas digitais, muitas vezes sem o conhecimento explícito do titular dos dados

O caso *Cambridge Analytica*[45] ilustra o potencial de manipulação em larga escala quando dados pessoais são utilizados de forma não ética. Este incidente expôs como informações aparentemente triviais podem ser empregadas para influenciar comportamentos políticos e sociais, levantando questões sérias sobre a integridade democrática na era digital.

Esta prática reflete uma transformação profunda na concepção da identidade humana. Como observado pelo Stefano Rodotà, estamos testemunhando uma evolução onde os indivíduos não são mais percebidos apenas como entidades físicas, mas também como "corpos eletrônicos", conferindo vantagem competitivas aos empreendimentos que adotam essa técnica a algoritmização da vida. Uma nova concepção transcende a materialidade física, incorporando uma dimensão digital que é constantemente atualizada e reinterpretada por algoritmos. Como resultado, as pessoas são cada vez mais percebidas e avaliadas com base em seus rastros digitais, muitas vezes sem plena consciência das implicações desta exposição (RODOTÀ, 2008).

Neste contexto, as pessoas são constantemente classificadas e categorizadas com base em inferências sobre diversos aspectos de sua personalidade. Estas categorizações servem como base para decisões automatizadas que visam antecipar ou influenciar preferências, gostos e comportamentos individuais.

Ressaltando que as interações cotidianas são transformadas em dados que alimentam sistemas preditivos, criando um ciclo de retroalimentação entre comportamento e previsão.

Assim, emerge um cenário onde nossas *personas digitais*[46] ganham cada vez mais relevância, influenciando decisões que afetam nossas vidas reais, desde oportunidades de emprego até acesso a serviços e produtos. A autonomia individual é potencialmente comprometida quando decisões importantes são tomadas com base em inferências algorítmicas, muitas vezes opacas e incompreensíveis para os indivíduos afetados. Além disso, a privacidade, como direito fundamental, é desafiada pela coleta e análise ubíqua de dados pessoais (NISSENBAUM, 2010).

---

[44] A raspagem de dados, em sua forma mais geral, é uma técnica na qual um programa de computador extrai dados dos resultados gerados por outro programa. A raspagem de dados geralmente se manifesta na forma de raspagem da internet, que é o processo de usar um aplicativo para extrair informações valiosas de um site.

[45] O caso *Cambridge Analytica* será aprofundado mais a frente.

[46] *Personas digitais* são personagens fictícios que representam o cliente ideal de uma empresa, produto ou serviço. Elas são criadas com base em dados e características de clientes reais, como comportamentos, preferências, problemas, desafios e objetivos.

Embora os perfis algorítmicos ofereçam benefícios inegáveis em termos de eficiência e personalização, como destacado por Mireille Hildebrandt, se faz importante reconhecer os riscos associados. A padronização excessiva de comportamentos, a perpetuação de vieses e a potencial discriminação são preocupações reais que exigem atenção e regulamentação adequadas, podendo restringir a liberdade individual e o desenvolvimento pessoal, ao reduzir indivíduos a um conjunto fixo de preferências e comportamentos observados em um momento específico. Isso pode levar à desconsideração de nuances individuais e à cristalização de perfis historicamente determinados (HILDEBRANT, 2008; DONEDA, 2021; RODOTÀ, 2008).

A analogia da 'borboleta-de-pequim', proposta pelos teóricos do caos, oferece uma perspectiva valiosa para compreender a complexidade e a imprevisibilidade dos sistemas sociais contemporâneos, especialmente no contexto da era digital. Esta metáfora ilustra como pequenas variações nas condições iniciais podem levar a consequências de larga escala e difíceis de prever, um fenômeno particularmente relevante no âmbito da análise de dados e tomada de decisões automatizadas.

No cenário atual, onde bilhões de decisões são tomadas diariamente com base em análises algorítmicas, a sensibilidade a condições iniciais torna-se ainda mais pronunciada. A interação entre sistemas complexos de processamento de dados e o comportamento humano cria um ambiente onde a previsibilidade é constantemente desafiada. Como observado por Adams, a introdução do elemento humano nestes sistemas adiciona uma camada extra de complexidade, pois as pessoas reagem às previsões, potencialmente alterando os resultados esperados:

> Diariamente, bilhões de decisões são tomadas. Na maioria dos casos, as consequências parecem ser apenas locais, mas talvez não sejam. Os teóricos do caos apresentam uma nova forma de inseto chamada 'borboleta-de-pequim' – o bater de suas asas em Pequim provoca uma sequencia de eventos que, após duas semanas, culmina com um furacão em Nova York. A sensibilidade extrema a diferenças sutis em condições iniciais – dizem os teóricos do caos – torna o comportamento dos sistemas naturais complexos inerentemente imprevisíveis. A previsão é ainda mais difícil quando as pessoas são introduzidas nesses sistemas – porque elas reagem à previsões, alterando assim o resultado previsto. Raramente as decisões sobre o risco são tomadas com informações que podem ser reduzidas a probabilidade quantificáveis, porém, de alguma forma, as decisões são tomadas. (ADAMS, 2009, p. 36)

Esta realidade ressalta a importância de uma abordagem cautelosa e ética no desenvolvimento e aplicação de tecnologias de IA e análise de dados. Os sistemas autônomos, capazes de correlacionar padrões e produzir novos conhecimentos, como descrito por Büchi *et al*, apresentam tanto oportunidades quanto riscos significativos, com o potencial de transformar

vastas quantidades de dados em insights valiosos, mas também podem reduzir a complexidade humana a meros padrões comportamentais, potencialmente comprometendo a dignidade e a autonomia individual (BUCHI *et al.,* 2020).

> A visão kantiana do ser humano como fim em si é desvirtuada por um instrumentalismo, cuja a base é a expropriação de nossa personalidade em prol de finalidades alheias. A realidade digital converte situações existenciais em uma nova propriedade baseada na despossessão da essência daquilo que nos define, através de uma nova modificação comportamental cujo legado de danos pode custar nossa própria humanidade. (NETTO; ROSENVALD; 2024, p. 17)

Além disso, existe o risco de penalização injusta para aqueles que não se enquadram nas categorias predefinidas, especialmente em casos de perfis não distributivos, onde a formação e uso desses grupos muitas vezes ocorrem sem o conhecimento do indivíduo.

O caso *Cambridge Analytica* representa um marco significativo na história da manipulação de dados pessoais para fins políticos, ilustrando os riscos associados ao uso indevido de informações privadas em larga escala. A empresa de consultoria política e análise de dados obteve dados pessoais de aproximadamente 87 milhões de usuários do Facebook através de um aplicativo de teste de personalidade chamado "This Is Your Digital Life", coletando informações não apenas dos usuários diretos, mas também de seus amigos na rede social, sem conhecimento ou consentimento explícito (CARDOSO, 2018).

Utilizando o modelo de personalidade "OCEAN" (Abertura, Conscienciosidade, Extroversão, Amabilidade e Neuroticismo), a *Cambridge Analytica* criou perfis psicológicos detalhados para direcionar conteúdo político personalizado, com o objetivo de influenciar comportamentos eleitorais em campanhas de alto perfil, incluindo a eleição presidencial dos Estados Unidos em 2016 e o referendo do *Brexit* no Reino Unido.

As implicações deste caso ultrapassam a violação da privacidade individual. O escândalo expôs vulnerabilidades críticas nos sistemas democráticos contemporâneos, demonstrando como técnicas avançadas de análise de dados podem ser empregadas para manipular a opinião pública em larga escala. Evidenciou-se a necessidade urgente de regulamentações mais robustas no campo da proteção de dados e da ética digital, catalisando debates globais sobre a responsabilidade das plataformas de mídia social, a transparência no uso de dados pessoais e os limites éticos da publicidade política direcionada.

Este episódio serve como um alerta contundente sobre os riscos potenciais associados ao uso inadequado de tecnologias de análise de dados em contextos políticos e sociais. Demonstra como práticas aparentemente inofensivas de coleta de dados podem ter ramificações

profundas, afetando não apenas a privacidade individual, mas também a integridade dos sistemas democráticos e a coesão social.

Em sua obra ‘A Era do Capitalismo de Vigilância’, a pesquisadora Shoshana Zuboff oferece uma análise crítica deste fenômeno. Zuboff introduz o conceito de ‘capitalismo de vigilância’, descrevendo como as empresas de tecnologia acumulam, analisam e segmentam informações através de algoritmos sofisticados. Neste novo paradigma, a experiência humana é tratada como matéria-prima gratuita, convertida em dados comportamentais frequentemente sem o consentimento explícito dos indivíduos (ZUBOFF, 2018).

Zuboff argumenta que este fenômeno representa uma nova forma de poder, caracterizada pela concentração de conhecimento e pelo potencial ameaça à democracia e à liberdade individual. Ela afirma:

> Nós reivindicamos a experiência humana como matéria prima gratuita para se pegar. Com base nessa reinvindicação, podemos ignorar considerações de direitos, interesses, consciência ou o entendimento dos indivíduos; com base na nova reinvindicação afirmamos o direito de pegar a experiência do indivíduo para convertê-la em dados comportamentais; nosso direito de pegar, baseado na nossa reinvindicação de matéria prima gratuita, nos confere o direito de possuir dados comportamentais derivados da experiência humana; nossos direitos de pegar e possuir nos confere o direito de saber o que o conteúdo dos dados nos revela; nossos direitos de pegar, possuir e saber nos conferem nossos direitos às condições que preservam nossos direitos de pegar, possuir, saber e decidir. (ZUBOFF, 2021, p. 210-211)

Esta análise de Zuboff destaca as implicações profundas e potencialmente perturbadoras do capitalismo de vigilância na sociedade contemporânea. À medida que este modelo se torna cada vez mais prevalente, surgem questões urgentes sobre privacidade, autonomia individual e o futuro da democracia na era digital.

Um aspecto fundamental dessas técnicas, como observado por Danilo Doneda, é a crescente dissociação entre as informações fornecidas pelo indivíduo - seja diretamente ou através de suas interações digitais - e os novos usos atribuídos a esses dados. Esta divergência entre a intenção original do compartilhamento de dados e sua utilização final levanta questões importantes sobre privacidade e consentimento informado. O fenômeno destaca a necessidade de uma reavaliação contínua dos conceitos tradicionais de privacidade e proteção de dados pessoais (DONEDA, 2021).

Sandra Wachter e Mireille Mittelstadt aprofundam esta discussão ao apontar que dados aparentemente inócuos podem, através de análises e inferências sofisticadas, revelar aspectos íntimos e privados que o titular dos dados não teria intencionado compartilhar. Esta capacidade de extrair informações sensíveis de conjuntos de dados aparentemente benignos representa um

desafio significativo para os marcos regulatórios existentes e para as expectativas de privacidade dos indivíduos (WACHTER; MITTESTADT,2019).

O objetivo final dessas técnicas avançadas de análise de dados é antecipar o comportamento de grupos específicos de indivíduos. Esta antecipação é fundamentada na análise meticulosa de dados históricos, que são utilizados para identificar e projetar padrões comportamentais. Com base nessas previsões, as empresas e organizações buscam oferecer conteúdo, serviços ou produtos que sejam estatisticamente relevantes para esses grupos-alvo.

Reconhecendo esses riscos, o Supremo Tribunal Federal, na ADI nº 6.387/2020[47], enfatizou a necessidade de que o tratamento de dados pessoais respeite as garantias constitucionais de liberdade individual, privacidade e livre desenvolvimento da personalidade. Neste contexto, o direito de acesso e compreensão desses dados e seus usos torna-se fundamental para a proteção desses direitos constitucionais.

O insumo para a construção destes perfis é coletado em plataformas digitais ou objetos conectados à internet, atraindo a aplicação das normas de proteção de dados. Esta realidade demanda uma reflexão crítica sobre os limites éticos e legais do uso de dados pessoais e do poder preditivo dos algoritmos.

Diante deste cenário complexo e desafiador, torna-se imperativo examinar como as legislações de proteção de dados, tanto internacionais quanto nacionais, abordam a questão do perfilamento. A próxima seção se dedica a analisar as previsões específicas sobre perfilamento no GDPR e na LGPD, buscando compreender como estas normativas procuram equilibrar os benefícios da tecnologia com a proteção dos direitos fundamentais dos indivíduos.

> A visão kantiana do ser humano como fim em si é desvirtuada por um instrumentalismo, cuja a base é a expropriação de nossa personalidade em prol de finalidades alheias. A realidade digital converte situações existenciais em uma nova propriedade baseada na despossessão da essência daquilo que nos define, através de uma nova modificação comportamental cujo legado de danos pode custar nossa própria humanidade. (NETTO; ROSENVALD; 2024, p. 17)

A análise do perfilamento digital e suas implicações éticas e jurídicas evidencia a necessidade urgente de mecanismos efetivos para proteger os direitos dos titulares de dados no

[47] A Ação Direta de Inconstitucionalidade (ADI) 6.387/2020 foi um julgamento do Supremo Tribunal Federal (STF) que reconheceu o direito fundamental à proteção de dados pessoais. Ocorrei em maio de 2020 quando o STF referendou a medida cautelar que suspendeu a Medida Provisória 954/2020, a Medida Provisória 954/2020 previa o compartilhamento de dados de milhões de usuários de telefonia móvel e fixa com o IBGE. A decisão do STF foi influenciada pela Volkszählunsurteil, uma decisão do Tribunal Constitucional Federal Alemão de 1983, que reconheceu o direito à autodeterminação informativa. A decisão do STF consolidou o dado pessoal como merecedor de tutela constitucional, afastando a ideia de que existem dados pessoais neutros. A decisão do STF reforçou o mérito da PEC nº 17/19, que aguarda apreciação da Câmara dos Deputados (STF, 2020).

contexto das decisões automatizadas. Neste cenário, o direito à explicação emerge como uma ferramenta fundamental para promover a transparência e accountability algorítmica. O próximo capítulo examina como este direito se manifesta no ordenamento jurídico brasileiro, começando por suas raízes no CDC e na Lei do Cadastro Positivo, até sua atual configuração na LGPD. Especial atenção será dada ao precedente estabelecido pelo STJ no julgamento do Recurso Especial nº 1.419.697-RS, que, ao abordar a legitimidade dos sistemas de *credit scoring*, antecipou importantes discussões sobre transparência algorítmica. Em seguida, o capítulo analisa as diferentes dimensões do direito à explicação na LGPD, incluindo seus aspectos preventivos e reativos, bem como sua relação com a responsabilidade civil. Por fim, examina-se as propostas legislativas em curso que visam fortalecer este direito, oferecendo uma visão prospectiva de sua evolução no contexto brasileiro.

5 DIREITO À EXPLICAÇÃO NO DIREITO BRASILEIRO

O direito à explicação no ordenamento jurídico brasileiro desenvolveu-se gradualmente, acompanhando a evolução das tecnologias e das relações sociais. este desenvolvimento pode ser observado através de diferentes marcos normativos que, embora não tenham sido originalmente concebidos para regular decisões automatizadas, estabeleceram importantes fundamentos para a proteção dos direitos dos indivíduos frente a processos decisórios cada vez mais complexos. O CDC, como primeira legislação a abordar aspectos relacionados à transparência e ao direito à informação nas relações de consumo, representa um ponto de partida fundamental para a compreensão da construção do direito à explicação no Brasil. Sua análise permite identificar os alicerces sobre os quais se edificaram as posteriores garantias relacionadas à explicabilidade de decisões automatizadas, evidenciando uma progressiva preocupação do legislador com a proteção dos direitos fundamentais no contexto tecnológico.

5.1 Notas sobre o direito à explicação no CDC

Apesar do direito à explicação não ser tão claro no CDC, quanto nas normas publicadas posteriormente (que serão estudas neste capítulo), a sua existência no ordenamento jurídico pode ser percebida do estudo e análise do texto consumerista. Revelando a preocupação do legislador em garantir não apenas o acesso a informações, mas também sua compreensibilidade pelo consumidor, o que fundamenta a existência de um direito à explicação no ordenamento jurídico consumerista, especialmente relevante no contexto atual de decisões automatizadas

A priori, este trabalho deve retratar que o CDC recebeu influência dos estudos sobre perfilização iniciados nos Estados Unidos. As crescentes técnicas de perfilização, em 1960, mobilizaram acadêmicos americanos a estudarem sobre as relações com privacidade, informação e direito de compreensão da existência das bases de dados. Como consequência, em 1967, reportaram a *Association of Credit Bureaus of America*[48] (ACBA) a existência de 110 milhões de dossiês de consumidores, emitindo quase 100 milhões de relatórios.

[48] A *Association of Credit Bureaus of America* (ACBA) é uma organização que representa os birôs de crédito dos Estados Unidos. Esses birôs são responsáveis por coletar e manter informações sobre o histórico de crédito de consumidores e empresas, que são usadas para a criação de relatórios de crédito. Esses relatórios são solicitados por instituições financeiras, empresas e outras entidades para avaliar o risco de crédito antes de conceder empréstimos, emitir cartões de crédito ou tomar decisões financeiras. A ACBA atua como uma associação que representa os interesses de seus membros, promovendo boas práticas no setor, padronização de procedimentos e advocacy sobre políticas que afetam os birôs de crédito e o sistema de crédito dos EUA. Ela também pode oferecer serviços de pesquisa, educação e networking para seus membros.

Este foi o ponta-pé inicial para que a sociedade civil norte americana se preocupasse "sobre a exatidão desses relatórios, as técnicas de coleta de dados dos birôs de crédito, e a relevância das informações contidas nesses relatórios para os propósitos pelos quais eles foram requisitados" (FINK, 1972, p. 1291).

Enquanto em 1971, a *American Civil Liberties Union,* publicou o artigo intitulado 'a invasão dos dossiês', do autor Ralph Nader, alertou sobre os pontos discriminatórios e que lesionavam os direitos coletivos destes dossiês:

> Quando você busca um empréstimo de dinheiro, o concedente recebe um arquivo do birô de crédito para estabelecer sua pontuação de crédito. Esse dossiê contém todos os fatos pessoais que o birô de crédito pode reunir – seu emprego, salário, tempo em que está no atual emprego, status marital, uma lista de seus débitos passados e atuais, seu histórico de pagamento, qualquer registro criminal, ações judiciais de qualquer tipo e registros de imóveis em seu nome. O dossiê performance e até mesmo um teste de Q.I. que você fez no ensino médio. Quando a concedente terminar de conversar com o birô de crédito, ele provavelmente saberá mais sobre sua vida pessoal que sua sogra. [...] Birôs de crédito e agências de inspeção são as maiores fontes de informações sobre indivíduos. Mas governos, escolas, empregadores e bancos também são registradores, e algumas vezes fornecedores, de informação (ZANATTA, 2019, p. 10).

Arthur Miller é um outro autor que questionou os "direitos a privacidade individual que os cidadãos teriam diante de empresas especializadas em análise de perfis de consumidores" (ZANATTA, 2019, p. 10).

Estes estudos criaram na sociedade norte americana o debate sobre a "a impossibilidade de registros de certos tipos de informações e a necessidade de direitos básicos de acesso, informação e transparência" (ZANATTA, 2019, p. 10).

Os reflexos políticos deste discurso no mundo acadêmico iniciaram em 1969, quando o Senador Willian Proxmire, organizou audiências públicas para elaboração do projeto de lei de regulação do "mercado de informação", recebendo o nome de *Fair Credit Reporting Act*[49].

Nestes debates foram identificadas as três principais preocupações dos consumidores detidos pelos birôs de crédito. A primeira era das informações imprecisas, decorrentes dos erros na elaboração dos relatórios frutos das informações trocadas, enviesadas, desatualizadas, incompletas maliciosas e erros de computadores. Como consequência, dificuldade em corrigir registros incorretos, foram identificadas ausências de canais para correção, custos, bloqueios e obstáculos. Em terceiro, informações irrelevantes, mesmo que alguns atos tenham sido

[49] O *"Fair Credit Reporting Act"* é uma lei que visa proteger os dados dos cidadãos dos Estados Unidos (LOBO JUNIOR, 2020).

prescritos pela legislação americana, ainda constavam nas bases de dados, como ofensas de menor potencial ofensivo, ou sexualidade, escolhas morais e estilo de vida (HARPER, 2011).

Assim, conclui-se, pela pesquisa do autor Alan Westin em seu livro *Privacy and Freedom* (1967)[50], que os remédios presentes no ordenamento jurídico americano eram insuficientes para resolução dos problemas gerados pela indústria das fichas de crédito (ZANATTA, 2019).

Até aquele momento, os tribunais estadunidenses posicionavam-se que o direito ao acesso às informações só seriam possíveis caso demonstrado a ocorrência de danos. Com a finalidade de demonstrar os riscos sociais de posições como estas, Westin, durante as audiências públicas, destacou os riscos de uma "sociedade baseada em dossiês e registros", principalmente, em quando vislumbra-se as tendências da tecnologia da informação, pleiteando por um direito regulatório de matriz econômica e consumerista, estimulando a responsabilização civil pelos instrumentos tradicionais do *tort law*[51]. Portanto, a tutela do direito de acesso e controle dos dados pelos birôs, "incluindo um elemento de justiça (*fairness*) no modo como os dados poderiam ser tratados por computadores, ao invés de manter uma espécie de 'acesso à justiça' para uma pequena elite capaz de contratar advogados e levar casos à justiça", deveria ser prevista em lei. (WESTIN, 1967; ZANATTA, 2019, p. 12)

> Para que tal sistema funcione, eu acho que é necessário para sua aceitação que uma pessoa que tenha acesso ao seu arquivo concorde em não processar a empresa caso encontre um erro. Isso pode parecer uma imunização dos birôs de crédito em caso de erros, mas eu acho que o objetivo primário de nossa sociedade, na era do aprofundamento de julgamentos sobre indivíduos baseados em dossiês, é garantir o acesso aos arquivos e a correção de erros, ao invés de promover um método tradicional de responsabilidade por meio da ação de reparação [*responsibility-through-damage-suit*] (ZANNATA apud HARPER, 2011, p. 20).

A partir desta argumentação, o *Fair Credit Reporting Act* foi assinado em outubro de 1970, criando um conjunto de direitos básicos aos consumidores, como:

> (i) o direito de acesso às fontes das informações constantes em bancos de dados detidos por birôs de crédito, (ii) o direito de saber se informações nos arquivos foram usados por terceiros para "ação adversa contra a pessoa", (iii) o direito de obter uma

[50] Destaca-se que esta é uma das obras mais importantes da teoria contemporânea de privacidade. O *Privacy and Freedom* foi uma encomenda do "Comitê Especial de Ciências e Direito" Ordem dos Advogados de Nova Iorque, com apoio financeiro da Carnegie Corporation (DONEDA, 2021, p. 14-15).

[51] O termo *tort law* pode ser traduzido (tradução livre) como a lei de responsabilidade civil. Dentro do direito privado norte americano que estuda os atos ilícitos na esfera civil se chama tort law, e objetiva estudar as formas de responsabilização à vítima, por meio de uma ação judicial, muito embora os Tribunais, por vezes, reconheçam outras formas de reparação à vítima. As principais fontes da tort law em que são estabelecidos os tipos de conduta que contarão como ato ilítico, via de regra, abrangem enunciados em pareceres escritos por juízes no curso de ações judiciais particulares e também em leis e em regulamentos de agência ligada ao governo (ATZ, 2022).

> abertura do arquivo gratuita (*file disclosure*) uma vez por ano e quantas vezes for necessário em condições específicas (se a pessoa foi vítima de roubo de identidade, se é beneficiária de assistência pública, se está desempregada), (iv) o direito de saber qual a pontuação de crédito (*credit score*) derivada do banco de dados, (v) o direito de contestar uma informação incompleta ou incorreta, (vi) o direito de remover ou corrigir informações incorretas em 30 dias, (vii) o direito de não ter informação negativa computada por mais de sete anos (ZANATTA, 2019 p. 12).

Toda está discursão influenciou as pesquisas de juristas brasileiros que se encarregavam de elaborar o CDC, materializando no artigo 43[52] do Código Consumerista, que criou seis regras básicas:

> Primeiro, que o consumidor tem direito de acesso *às informações existentes* sobre ele, "bem como as respectivas fontes". Segundo, que os cadastros de consumidores devem ser verdadeiros e devem ter "linguagem de fácil compreensão". Terceiro, que a abertura dos registros e fichas de consumo "devem ser comunicadas ao consumidor". Quarto, que o consumidor possui o direito de corrigir informações inexatas, devendo o arquivista comunicar as alterações "aos eventuais destinatários" no prazo de "cinco dias úteis". Quinto, que as informações negativas sobre consumidores (*e.g.* registro de dívidas e contas não pagas) não podem ser registradas "a período superior a cinco anos". Sexto, que os "bancos de dados e cadastros relativos a consumidores e os serviços de proteção ao crédito" são considerados "entidades de caráter público" (ZANNATA, 2019, p. 13)

A legislação consumerista brasileira, embora não aborde especificamente a prática de perfilização, estabelece garantias fundamentais relacionadas ao tratamento de dados pessoais. O CDC assegura direitos essenciais como o acesso, a informação e a retificação dos dados, evidenciando uma preocupação com a proteção da privacidade e autodeterminação informativa do consumidor.

Observa-se uma notável convergência entre os debates desenvolvidos nos Estados Unidos e os direitos consagrados na legislação brasileira de proteção ao consumidor. Esta aproximação se manifesta especialmente nas obrigações relacionadas à boa-fé e ao dever de informação, princípios que se aplicam tanto à gestão de bancos de dados quanto aos métodos de avaliação de risco, incluindo os sistemas de pontuação creditícia (ZANATTA, 2019, p.15).

---

[52] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito (BRASIL, 1990).

Esta base normativa estabelecida pelo CDC, influenciada pela experiência norte-americana, mostrou-se ainda mais relevante com o advento das tecnologias digitais. A partir da década de 1990, com a popularização da internet, as relações de consumo passaram por uma profunda transformação, apresentando novos desafios para a proteção dos direitos do consumidor. Se anteriormente as preocupações centravam-se principalmente nos registros de dados por birôs de crédito, o ambiente digital multiplicou exponencialmente as possibilidades de coleta, processamento e utilização de dados pessoais.

No novo contexto, os princípios do CDC - como a boa-fé, transparência e direito à informação - precisaram ser reinterpretados e aplicados a situações cada vez mais complexas. A evolução tecnológica não apenas modificou a forma como os consumidores acessam produtos e serviços, mas também criou novas modalidades de tratamento de dados pessoais, tornando ainda mais crítica a necessidade de proteção efetiva dos direitos do consumidor.

Neste sentido, José Faleiros Junior e Filipe Medon destacam que "a doutrina dos contratos eletrônicos surgiu para garantir a observância a preceitos tradicionais da disciplina da contratualística em novos formatos", e portanto, não é permitido desviar o olhar dos "desafios igualmente novos e decorrentes de ilegalidades e abusividades que foram sendo enfrentados ao longo de mais de duas décadas de existência do CDC exatamente para que a disciplina jurídica pudesse manter sua higidez, em observância à almejada confiança" (FALEIROS, MEDON, 2021, p. 960).

Os contratos eletrônicos são categorizados como um dos "desdobramentos integrados ao ordenamento pela boa-fé objetiva em sua triple função". Todas as peculiaridades que rodeiam o tema, fez cunhar a nomenclatura "ciber-consumidor[53]" para se referir aquele que

[53] A evolução do comércio eletrônico e a crescente digitalização das relações de consumo têm suscitado a necessidade de uma terminologia específica para descrever o consumidor que atua no ambiente virtual. Neste contexto, surge o conceito de "ciber-consumidor" ou "consumidor internauta", termos que buscam capturar a especificidade das transações realizadas através da Internet. A origem desta expressão pode ser traçada à doutrina portuguesa, tendo sido notavelmente elaborada por Elsa Dias Oliveira. Em sua obra, Oliveira oferece uma definição concisa e elucidativa, descrevendo o ciber-consumidor como aquele que "celebra contratos através da Internet [...], [é] correntemente designado por consumidor internauta ou por ciber-consumidor". Esta conceituação inicial estabelece uma base fundamental para compreender a natureza distintiva do consumidor no ambiente digital. No contexto brasileiro, a introdução e disseminação deste termo podem ser atribuídas ao trabalho pioneiro de Claudia Lima Marques. Baseando-se nos estudos de Thibault Verbiest, Marques contribuiu significativamente para a incorporação desta terminologia no léxico jurídico nacional. A adoção deste termo por uma jurista de renome como Marques demonstra a relevância e a necessidade de se considerar as particularidades do consumo online no âmbito do direito do consumidor brasileiro. Complementando estas perspectivas, Pedro Modenesi oferece uma definição mais detalhada e assertiva do ciber-consumidor. Segundo Modenesi, o ciber-consumidor é "o civil ou leigo que adquire produto ou serviço, pela Internet, de um fornecedor (empresário ou profissional)". Esta definição é particularmente valiosa por sua precisão, destacando elementos importantes como a natureza leiga do consumidor, a aquisição de produtos ou serviços, o meio utilizado (Internet) e a caracterização do fornecedor como entidade profissional ou empresarial. A conceituação proposta por Modenesi é especialmente relevante no contexto jurídico atual, pois abrange aspectos fundamentais das relações de consumo online. Ao enfatizar a condição de "civil ou leigo" do consumidor, ela reafirma a vulnerabilidade

"firma contratos eletrônicos de consumo". Todo o contexto de tutela toma contorno ainda mais desafiadores com a utilização de algoritmos de IA (MARTINS, 2016; FALEIROS; MEDON, 2021; GOETTENAUER, 2019).

Neste sentido posiciona-se a autora Lauren Scholz:

> Esta abordagem, para avaliar contratos algorítmicos, apresenta resultados melhores ao atingir as metas de redução de externalidades e preservação do jogo justo no comércio do que no *status quo* ambíguo de ignorar contratos algorítmicos como uma categoria especial de acordos. A abordagem faz isso ao mesmo tempo em que faz jus às ações e riscos assumidos pelas partes do acordo. Dito de outra forma, esta abordagem multifacetada para contratos algorítmicos permite que a lei mantenha acordos algorítmicos quando eles são feitos de forma justa, mas produz reequilíbrio justamente quando eles não são (SCHOLZ,2017, p. 167).

Os direitos ao ciber-consumidor foram assegurados e confirmados pelo STJ em 2014 no julgamento do Recurso Especial 1.419.697/RS – objeto da primeira audiência pública da história do STJ –, o ministro Paulo de Tarso Sanseverino decidiu que os sistemas de pontuação de crédito, mesmo não sendo "banco de dados" em sentido estrito, devem ser tratados com o máximo de transparência e boa-fé na relação com os consumidores, aplicando-se os princípios do CDC e os direitos básicos do art. 5º da Lei 12.414/2011, que será estudado no tópico 5.3 deste trabalho.

O tratamento do direito à explicação no CDC estabeleceu importantes bases para a proteção dos consumidores em face de decisões automatizadas. Contudo, foi com o advento da Lei do Cadastro Positivo que o ordenamento jurídico brasileiro começou a desenvolver instrumentos mais específicos para lidar com a complexidade do tratamento automatizado de dados pessoais. Esta legislação representou um avanço significativo ao estabelecer garantias mais robustas para os titulares de dados, especialmente no contexto das análises de crédito. A relevância desta evolução normativa seria posteriormente evidenciada no emblemático julgamento do Recurso Especial nº 1.419.697/RS pelo Superior Tribunal de Justiça, que, ao

---

intrínseca deste agente nas transações digitais, alinhando-se com os princípios fundamentais do direito do consumidor. Ademais, ao especificar a Internet como meio de aquisição, esta definição demarca claramente o escopo das transações em questão, diferenciando-as das formas tradicionais de comércio. É importante ressaltar que a evolução deste conceito reflete as mudanças significativas nas dinâmicas de consumo propiciadas pela revolução digital. O ciber-consumidor enfrenta desafios únicos, como a desmaterialização das transações, a complexidade dos termos de uso de plataformas digitais, e questões relacionadas à segurança e privacidade de dados. Portanto, a adoção e refinamento deste termo não são apenas exercícios acadêmicos, mas respondem a uma necessidade prática de adaptar o arcabouço legal e conceitual às realidades do comércio eletrônico. Em suma, o desenvolvimento do conceito de ciber-consumidor, desde sua introdução na doutrina portuguesa até sua elaboração mais recente por juristas brasileiros, representa um importante avanço na compreensão e regulação das relações de consumo no ambiente digital. Este conceito fornece uma base sólida para a análise jurídica e a formulação de políticas públicas que visam proteger os direitos dos consumidores no contexto específico do comércio eletrônico, reconhecendo suas particularidades e desafios únicos (OLIVEIRA, 2002, p. 57; MARQUES, 2004; MODENESI, 2021, p. 564).

analisar a legitimidade dos sistemas de *credit scoring*, consolidou importantes entendimentos sobre transparência algorítmica e direito à explicação. Assim, antes de examinarmos este precedente judicial transformador, é fundamental compreender como a Lei do Cadastro Positivo estabeleceu o arcabouço normativo que influenciaria tanto a decisão do STJ quanto o posterior desenvolvimento da LGPD.

5.2 Notas sobre o direito à explicação na Lei do Cadastro Positivo

Durante 21 (vinte e um) anos, a tutela a coleta de dados pessoais e formação dos bancos de dados eram previstos no CDC e em normas setoriais, como a Lei Geral de Telecomunicações[54]. Este cenário sofreu alteração em 2011, quando da aprovação da Lei 12.414, trazendo regulamentações sobre o "cadastro positivo".

Leonardo Bessa expõe que a legislação apresentou um rol de direitos básicos dos cadastrados, indo além do acesso à informação ou retificação, aproximando com preocupações com análises de juízos de valor a partir do "perfil digital" e suas consequências, como "transferências não autorizadas, tratamentos discriminatórios e acesso a informações sensíveis". Havendo limites jurídicos ao conceito de "bons pagadores" contra informações excessivas e sensíveis:

> As vedações de informações sensíveis e excessivas visam mitigar a potencialidade ofensiva dos bancos de dados ao direito à privacidade. O dispositivo, que merece elogios, recebeu influência da Diretiva 95/46 da União Europeia. O art.6º da Diretiva estipula que os dados devem ser adequados, pertinentes e *não excessivos* em relação ao propósito para os quais foi colhido. Mais à frente, no art. 8º, a Diretiva prescreve que os Estados-membro da União Europeia proibirão, com algumas exceções, o tratamento dos dados sensíveis, que são aqueles reveladores de origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, estado de saúde e opções sexuais. [...] A Lei 12.414/2011 veda o tratamento de informações excessivas. Se pode ser verdadeiro, sob a ótica econômica, quanto mais informações melhor é a avaliação de crédito (*more is better*), para o direito, para proteção jurídica da privacidade, é fundamental restringir, tanto no tempo, como na qualidade e quantidade, as informações que circulam pelos bancos de dados de proteção ao crédito. (BESSA, 2014, p. 93/94).

A legislação foi inovadora por destacar a necessidade de consentimento para ingressar nas relações contratuais que organizam o cadastro positivo, como consequência apresentou "uma dupla preocupação para dentro do sistema jurídico com relação aos tipos de dados que poderiam ser utilizados (ZANATTA, 2019).

[54] Lei nº 9.472/1997.

A primeira, prevista no art. 3º, §3º, II[55] da Lei 12.414/11, consiste na proteção dos dados sensíveis, elencados na legislação como aqueles que tratam sobre "origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas", utilizados com a finalidade de credito (BRASIL, 2011).

Em seguida, preocupou-se com a necessidade[56] do dado para histórico de crédito ou cumprimento de obrigação legal.

Nesse sentido, a legislação prevê, pioneiramente, em seu art. 5º, o direito de revisão de decisões exclusivamente automatizadas, "já considerando a existência de um amplo sistema de "clusterização[57]" e de perfilização para fins de crédito iniciado na década de 1970" (ZANATTA, 2019, p.17).

Neste sentido a Lei de Cadastro Positivo, em seu art. 5ª estabelece que:

> Art. 5º. São direitos do cadastrado:
> I - Obter o cancelamento ou a reabertura do cadastro, quando solicitado;
> II - Acessar gratuitamente, independentemente de justificativa, as informações sobre ele existentes no banco de dados, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado;
> III - Solicitar a impugnação de qualquer informação sobre ele erroneamente anotada em banco de dados e ter, em até 10 (dez) dias, sua correção ou seu cancelamento em todos os bancos de dados que compartilharam a informação;
> IV - Conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial;
> V - Ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais;
> VI - Solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados; e
> VII - Ter os seus dados pessoais utilizados somente de acordo com a finalidade para a qual eles foram coletados (BRASIL, 2011).

Por este motivo, os autores Renato Leite Monteiro, Maria Cecília Oliveira e Bruno Bioni posicionam-se no sentido de que a norma do cadastro positivo foi a precursora da LGPD, sendo tão somente adaptado:

---

[55] Art. 3º. Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei. [...] § 3º. Ficam proibidas as anotações de: [...] II - informações sensíveis, assicm consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas.

[56] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

[57] Clusterização é uma técnica de *machine learning* que agrupa dados semelhantes em grupos, chamados de clusters. É um método não supervisionado, ou seja, não requer um conjunto de dados rotulados para ser aplicado (TOTVS, 2024).

> O direito de uma revisão por uma pessoa natural de tomada de decisão automatizada que impacta os titulares de dados (Art. 22) não é novo para o sistema legal brasileiro. Ele foi fornecido em relação aos modelos de *credit scoring* pela Lei do Cadastro Positivo juntamente com o direito à explicação, que incluiria não apenas os dados usados pelo algoritmo, mas também os critérios usados para processamento, limitados ao sigilo comercial e levando em consideração direito de propriedade intelectual. Essa estrutura foi totalmente copiada pela LGPD, mas aplicável para processamento de dados para qualquer finalidade. No entanto, comparado com o GDPR, o impacto sobre o titular dos dados é presumido quando a tomada de decisão automatizada se baseia na criação de perfis (*profiling*), e não há limitação para situações em que os dados foram fornecidos por consentimento (BIONI; MONTEIRO; OLIVEIRA, 2018).

Complementando, o Rafael Zanatta afirma que esta não é uma norma proibitiva geral ao *profiling*, entretanto, "mas sim a atribuição de um direito de revisão automatizada que permite a fruição do direito de não discriminação previsto no art. 3º". O que representa ser "instrumental para a identificação de potenciais violações de direitos", como por exemplo, o uso de dados para avaliação de risco conforme o endereço.[58] (ZANATTA, 2019, p. 18)

> É por meio do direito básico do art. 5º, VI, que, teoricamente, um cidadão cadastrado pode identificar se, mesmo com um hábito regular de pagamentos de contas e higidez financeira, ele está sendo discriminado "em grupo" por morar em bairro periférico de São Paulo (o que levaria o sistema de clusterização usado pelo birô de crédito a *inferir* que aquela pessoa possui um risco mais elevado de crédito pelo simples fato de residir em uma localização onde, de acordo com análise estatística, há um grande número de "maus pagadores"). (ZANATTA, 2019, p. 19)

A decisão do STJ estudada no tópico anterior, caminhou no sentido previsto na norma:

> É evidente que os birôs de crédito podem criar metodologias de análise de risco dentro e fora do Cadastro Positivo – há liberdade empresarial para criação de diferentes metodologias de análise de risco –, porém os entes privados precisam assumir compromissos de (i) *garantia de informação* sobre quais dados compõem as bases do sistema de pontuação e (ii) *não discriminação abusiva*, podendo ser responsabilizadas civilmente por danos morais (de forma objetiva) pelo fato de utilizarem informações sensíveis e informações excessivas (ZANATTA, 2019, p. 19).

A análise da Lei do Cadastro Positivo revela sua função exemplar no ordenamento jurídico brasileiro quanto à proteção de dados pessoais. Ao estabelecer direitos fundamentais como o consentimento do titular, a proteção contra dados sensíveis e excessivos, e especialmente o direito à explicação de decisões automatizadas, a lei inaugurou uma nova referência na regulação do tratamento de dados no país. Esta inovação normativa se manifesta em três aspectos principais: primeiro, na preocupação com a transparência dos critérios utilizados para análise de risco; segundo, na garantia do direito à revisão de decisões

[58] Esta prática é denominada de *geo pricing* e *geo blocking* e consideram a localização geográfica para precificação algorítmica, mas com nuances próprias. (FALEIROS; MEDON, 2021, p. 955).

automatizadas; e terceiro, na proteção contra práticas discriminatórias derivadas do tratamento de dados.

Mais do que um marco setorial voltado exclusivamente para relações creditícias, a Lei do Cadastro Positivo funcionou como um importante laboratório jurídico que pavimentou o caminho para uma regulamentação mais abrangente e sistemática. Os princípios e direitos nela estabelecidos foram posteriormente expandidos e aprofundados pela LGPD, que estabeleceu um marco regulatório mais amplo transcendendo o contexto específico do cadastro positivo. Esta evolução normativa demonstra como a experiência setorial contribuiu decisivamente para o amadurecimento do sistema brasileiro de proteção de dados pessoais, representando uma evolução na proteção dos direitos dos titulares de dados no Brasil e alinhando o país às melhores práticas internacionais de proteção de dados.

A análise da Lei do Cadastro Positivo demonstra como o ordenamento jurídico brasileiro começou a desenvolver mecanismos específicos para proteger os titulares de dados em contextos de decisões automatizadas. Esta evolução normativa seria colocada à prova em um dos casos mais emblemáticos sobre o tema no judiciário brasileiro: o julgamento do Recurso Especial nº 1.419.697/RS pelo STJ. Este precedente, que se tornou um divisor de águas na jurisprudência nacional, não apenas interpretou a aplicação prática da Lei do Cadastro Positivo, mas também estabeleceu parâmetros fundamentais para a transparência algorítmica no contexto das análises de crédito. O caso, que culminou na primeira audiência pública da história do STJ, representa um momento crucial na construção jurisprudencial do direito à explicação no Brasil, antecipando diversos aspectos que seriam posteriormente incorporados pela LGPD.

5.3 ADIN – Recurso Especial nº 1.419.697 - RS (2013/0386285-0)

O presente trabalho analisa o Recurso Especial nº 1.419.697, julgado pelo STJ, que aborda a legalidade dos sistemas de *credit scoring* sob a perspectiva do CDC. O caso, envolvendo a empresa Boa Vista Serviços S/A, questiona uma decisão do Tribunal de Justiça do Estado do Rio Grande do Sul sobre a utilização de dados dos consumidores para avaliação de risco de crédito. O objetivo principal é determinar se esse sistema de pontuação infringe direitos básicos dos consumidores, como a privacidade e o direito à informação, e se gera dano moral passível de indenização.

Diante da complexidade e relevância deste caso, a escolha deste recurso especial como objeto de estudo justifica-se por quatro aspectos fundamentais: seu pioneirismo ao abordar questões relacionadas a decisões automatizadas no judiciário brasileiro; seu processamento sob

o rito dos recursos repetitivos, que estabeleceu um precedente vinculante em âmbito nacional; a abrangência sistemática de seu exame que contemplou sete dimensões do tema (desde o conceito de *credit scoring* até questões de dano moral); e sua relevância histórica para a evolução normativa brasileira, antecipando discussões que posteriormente seriam incorporadas pela LGPD, como transparência algorítmica e direito à explicação. Este julgado de 2013 estabeleceu importantes parâmetros para o equilíbrio entre as necessidades comerciais e a proteção dos direitos dos consumidores, mantendo-se atual mesmo diante das transformações tecnológicas e legislativas subsequentes.

Para compreender melhor o mérito da questão, a ação foi movida argumentando três violações principais: falta de transparência por não informar claramente os critérios de pontuação, violação à privacidade pela ausência de consentimento para uso dos dados pessoais, e dano moral pelo constrangimento causado pela negativa de crédito.

Em contraposição a estas alegações, a defesa da Boa Vista Serviços S/A baseou-se em três argumentos principais: ilegitimidade passiva por não ter controle sobre as decisões de crédito; natureza objetiva do sistema como ferramenta estatística; e conformidade com a legislação vigente, incluindo CDC e Lei do Cadastro Positivo.

Aprofundando seus argumentos, a empresa defendeu a objetividade do método, afirmando que o sistema não realiza análises subjetivas dos consumidores e que o procedimento adotado é similar ao utilizado por seguradoras e outras entidades financeiras para avaliar riscos.

Complementando sua defesa, afirma estar em conformidade com a legislação, incluindo o CDC e a Lei do Cadastro Positivo (Lei nº 12.414/2011), argumentou que o serviço de *credit scoring* é uma prática legal de mercado, usada para facilitar o estudo de risco e que respeita os direitos dos consumidores na medida em que utiliza dados disponíveis publicamente e adota critérios objetivos para a avaliação de risco de crédito.

Após a apreciação das argumentações apresentadas, a sentença de primeiro grau decidiu em desfavor da Boa Vista Serviços S/A. O juiz entendeu que o uso do sistema de *credit scoring* pela Boa Vista, especificamente o SCPC Score Crédito, violava direitos dos consumidores garantidos pelo CDC.

Na fundamentação do veredito considerou, ainda, que a prática de utilizar um sistema de pontuação de crédito com base em dados negativos dos consumidores, sem o devido consentimento e sem transparência sobre os critérios utilizados, era abusiva. O juiz entendeu que o sistema de *scoring* utilizado pela Boa Vista não fornecia informações claras e precisas aos consumidores sobre como suas pontuações eram calculadas e quais fatores eram

considerados. Essa falta de transparência foi vista como uma violação do direito à informação, um direito básico do consumidor.

Além da questão da transparência também reconheceu a existência de dano moral causado ao autor, concluindo que a prática de atribuir pontuações de crédito sem a devida clareza e sem a participação ativa dos consumidores na compreensão desse processo gerava frustração e ansiedade, especialmente quando resultava na negativa de crédito, portanto o dano moral era presumido ("*in re ipsa*") devido à violação dos direitos básicos do consumidor e ao impacto negativo dessa prática na vida pessoal e econômica do autor.

Aprofundando a verificação dos direitos violados o julgamento destacou que o uso de dados pessoais para fins de cálculo de risco de crédito, sem um consentimento claro e específico, violava o direito à privacidade dos consumidores, conforme estabelecido pelo CDC e pela CF. A sentença considerou que os consumidores deveriam ter o direito de saber como seus dados eram utilizados e quais informações estavam sendo consideradas na verificação de risco.

Em face deste entendimento, o acórdão do STJ decidiu, em parte, em favor da Boa Vista Serviços S/A, reformando parcialmente a manifestação judicial de instâncias inferiores. O STJ fez uma ponderação detalhada sobre a legalidade do sistema e os direitos dos consumidores no Brasil, definindo os limites e os requisitos necessários para a legalidade dessa prática.

No mérito da questão decidiu pela Legalidade do Sistema de *Credit Scoring*, como uma prática comercial para avaliar o risco de concessão de crédito. A corte considerou que o uso de modelos estatísticos para calcular a probabilidade de inadimplência é uma prática lícita desde que respeite os direitos dos consumidores, especialmente no que diz respeito à transparência e ao direito à informação.

Desenvolvendo este entendimento, o STJ decidiu parcialmente em favor da Boa Vista Serviços S/A, reconhecendo a legalidade do sistema de *credit scoring* como prática comercial legítima para avaliação de risco de crédito. A Corte estabeleceu que o uso de "modelos estatísticos para calcular probabilidade de inadimplência é lícito, desde que respeite os direitos dos consumidores, especialmente quanto à transparência e direito à informação. Como destacado anteriormente, este caso tornou-se paradigmático por seu pioneirismo em abordar questões relacionadas a decisões automatizadas no judiciário brasileiro, estabelecendo um precedente vinculante em âmbito nacional que anteciparia discussões posteriormente incorporadas pela LGPD.

Para operacionalizar esta deliberação determinou que as empresas que utilizam sistemas de pontuação de crédito devem: (1) disponibilizar de forma clara e acessível os critérios e

variáveis utilizados no cálculo da pontuação; (2) assegurar a veracidade das informações empregadas na avaliação; e (3) respeitar a privacidade e proteção de dados pessoais dos consumidores, garantindo-lhes o direito de acesso às informações e possibilidade de solicitar correções em caso de inexatidões

Para além dos aspectos práticos a relevância histórica deste entendimento para a evolução normativa brasileira se evidencia especialmente na forma como o Tribunal estabeleceu parâmetros para o equilíbrio entre necessidades comerciais e proteção dos direitos dos consumidores, afastando a presunção automática de dano moral. Para haver responsabilização por danos morais, passou a ser necessária a comprovação de abuso ou uso inadequado dos dados. Este julgamento serviu como precedente para avaliações posteriores sobre uso de IA em processos decisórios financeiros, antecipando discussões que seriam posteriormente incorporadas pela LGPD, como transparência algorítmica e direito à explicação.

Expandindo a ponderação para um contexto mais amplo esta decisão judicial serve como pano de fundo para uma interpretação mais ampla sobre o uso de IA em processos decisórios financeiros. A avaliação de concessão de empréstimos é uma das áreas essenciais para as instituições financeiras e que tem passado por transformações significativas com a implementação da robótica para auxiliar na definição dos perfis dos consumidores. Entre todos os benefícios que a tecnologia possui, encontramos a capacidade de processar grande volume de dados e identificar sutis padrões que permitem que os credores tomem decisões mais rápidas e precisas.

Retornando aos aspectos específicos do entendimento, em resposta específica à questão da transparência, o acórdão determinou que as entidades que empregam sistemas de pontuação de crédito têm a obrigação de disponibilizar, de forma clara e acessível, informações detalhadas sobre os critérios e variáveis utilizados no cálculo da pontuação creditícia. Esta determinação visou especificamente sanar a falta de clareza inicialmente apontada pelos consumidores, proporcionando-lhes uma compreensão mais aprofundada sobre como suas informações pessoais são processadas e avaliadas.

Um ponto particularmente controverso no processo é a questão do dano moral recebeu interpretações distintas nas diferentes instâncias. Em primeira instância, o juiz reconheceu o dano moral como presumido (*in re ipsa*), entendendo que a prática de atribuir pontuações de crédito sem transparência gerava frustração e ansiedade, especialmente quando resultava na negativa de crédito.

No entanto, esta interpretação não prevaleceu nas instâncias superiores, o STJ, contudo, adotou posicionamento diverso ao estabelecer que estas entidades não são automaticamente

responsáveis por danos morais. A Corte Superior afastou a presunção automática de dano, exigindo a comprovação concreta de abuso ou uso inadequado dos dados para fundamentar eventuais pedidos de indenização. Esta mudança de entendimento reflete uma abordagem mais equilibrada, que reconhece a legitimidade do sistema de *credit scoring* enquanto estabelece critérios mais rigorosos para a caracterização do dano moral.

Para ilustrar a complexidade desta questão na prática, um exemplo pertinente é o cenário de uma instituição financeira que implementa um sistema de IA para avaliar solicitações de empréstimo. Neste contexto, o algoritmo é projetado para prever a probabilidade de inadimplência dos solicitantes, determinando assim a aprovação ou rejeição dos pedidos de crédito (LEHR; OHM, 2017).

Contudo, esta aplicação não está isenta de desafios quando o treinamento deste algoritmo se baseia unicamente em dados históricos de clientes cujos empréstimos foram aprovados. Esta abordagem restritiva gera uma lacuna considerável na capacidade do sistema de avaliar adequadamente novos candidatos que poderiam ter suas solicitações negadas, uma vez que o modelo carece de exemplos destes casos em sua base de treinamento.

Esta problemática[59] ilustra uma questão mais ampla como a qualidade e a abrangência dos dados de treinamento impactam direta e substancialmente o desempenho e a equidade dos modelos de aprendizado de máquina. As implicações dessas limitações transcendem o setor financeiro, afetando diversos aspectos do cotidiano das pessoas.

A abrangência desta questão podemos analisar os modelos que podem ser espelhados em diversos contextos desde a concessão de crédito até diagnósticos médicos e experiências com aplicativos de uso diário. Cada uma dessas interações tem o potencial de afetar significativamente a vida dos indivíduos.

É importante ressaltar que, embora a qualidade dos dados seja um fator crítico, não é a única fonte de problemas associados aos algoritmos de aprendizado de máquina. A complexidade destes sistemas envolve múltiplos fatores que podem contribuir para resultados inadequados ou injustos.

Retomando ao estudo do caso em questão sob uma perspectiva temporal, a decisão judicial mencionada foi objeto de apreciação pelo Tribunal em 2013, utilizando como base legal o CDC. À época, não existiam as discussões sobre dados pessoais que culminaram na

[59] Um relatório produzido em abril de 2019 pelo AI Now Institute, um centro interdisciplinar dedicado à pesquisa sobre as implicações sociais da IA, compilou diversos casos que evidenciam discriminação, particularmente de gênero e raça, em produtos e programas de IA. Estas situações foram frequentemente motivadas pelos dados utilizados como input, ressaltando a importância crítica da qualidade e diversidade dos dados no desenvolvimento de sistemas de IA éticos e equitativos (WEST; WHITTAKER; CRAWFORD, 2019).

promulgação da LGPD, nem abordagens sobre perfilização e decisões automatizadas, apesar de já implementadas.

Considerando estas mudanças significativas faz-se necessário analisar o acordão à luz do novo cenário social, democrático, tecnológico e legislativo. É importante notar que, apesar da relevância do tema, poucos estudos se dedicaram a analisar esta temática em profundidade.

A relevância desta se intensifica, especialmente, considerando a LGPD trazendo novos parâmetros para a proteção de dados pessoais e a privacidade dos consumidores. A norma protetiva de dados reforça princípios fundamentais ao exigir que empresas que utilizam processos automatizados para tomada de decisões que impactam os direitos e interesses dos indivíduos forneçam explicações claras sobre esses processos. Essas explicações devem permitir que o indivíduo compreenda como suas informações pessoais foram utilizadas para chegar a uma determinada decisão. Isso inclui a divulgação dos principais elementos e critérios considerados na análise de risco de crédito, respeitando-se o segredo empresarial.

Esta evolução normativa, no contexto brasileiro, a posição adotada pelos Ministros do STJ e os princípios da LGPD alinham-se com a tendência internacional de aumentar a transparência e a responsabilidade nas decisões baseadas em dados

Aprofundando este estudo, a relação entre o *credit scoring* e os conceitos trazidos pela LGPD merece especial atenção, particularmente no que tange à perfilização e ao direito à explicação. O sistema de pontuação de crédito, ao processar dados pessoais para criar perfis de risco dos consumidores, enquadra-se diretamente no conceito de perfilização estabelecido pela LGPD, que compreende qualquer forma de tratamento automatizado de dados pessoais para avaliar aspectos da vida do titular, especialmente para analisar sua situação econômica.

Esta intersecção torna-se ainda mais relevante quando consideramos que o direito à explicação, previsto no art. 20 da LGPD, impõe às entidades que utilizam estes sistemas a obrigação de fornecer informações claras e acessíveis sobre a lógica por trás das decisões automatizadas. Assim, se no julgado do STJ de 2013 a transparência era fundamentada principalmente no CDC, agora encontra respaldo adicional e mais específico na LGPD, que vai além ao exigir não apenas a divulgação dos critérios utilizados, mas também a possibilidade de revisão das decisões por pessoa natural. Esta nova camada de proteção legal reforça a necessidade de que as empresas que operam sistemas não apenas informem as variáveis consideradas, mas também expliquem como estas influenciam o processo decisório, garantindo ao titular dos dados uma compreensão efetiva sobre como suas informações pessoais impactam sua pontuação de crédito, ressalvados os segredos comerciais e industriais.

Na prática, a aplicação do direito à explicação implica que as empresas que utilizam esses sistemas devem estar preparadas para fornecer informações claras e acessíveis sobre como os dados pessoais são utilizados para calcular a pontuação de risco de crédito e como essa pontuação influencia as decisões de concessão de crédito. Isso pode incluir a divulgação de variáveis específicas, modelos estatísticos utilizados e como as informações são coletadas e processadas.

Em uma perspectiva mais ampla, toda esta visão apresenta novas exigências e maior robustez à proteção de dados, refletindo nas tratativas que serão dadas ao direito à explicação. O conceito de *accountability*, mencionado anteriormente, será apresentado em detalhes em um tópico subsequente.

O julgamento do Recurso Especial nº 1.419.697/RS pelo STJ estabeleceu importantes balizas para a transparência algorítmica no contexto das análises de crédito, antecipando muitas das preocupações que viriam a ser centrais no debate sobre decisões automatizadas. No entanto, seria com a promulgação da LGPD que o direito brasileiro ganharia um arcabouço normativo mais abrangente e sistemático para lidar com estas questões. A LGPD não apenas incorporou e expandiu muitos dos princípios já reconhecidos pela jurisprudência do STJ, mas também estabeleceu um conjunto mais amplo de direitos e garantias aplicáveis a todas as formas de tratamento automatizado de dados pessoais. Esta nova legislação representa uma evolução significativa na proteção dos titulares de dados, oferecendo instrumentos mais robustos e específicos para garantir a transparência e explicabilidade das decisões automatizadas em diversos contextos, transcendendo o escopo inicial das análises de crédito.

5.4 Notas sobre o direito à explicação na LGPD

A Lei Geral de Proteção de Dados representa um marco significativo na regulamentação do tratamento de dados pessoais no Brasil, estabelecendo um sistema normativo abrangente que contempla tanto aspectos preventivos quanto reativos na proteção dos direitos dos titulares. A análise do direito à explicação no contexto da LGPD demanda, inicialmente, uma compreensão aprofundada de sua estrutura normativa e dos princípios que a fundamentam. Esta abordagem permite identificar como o direito à explicação se integra ao conjunto mais amplo de garantias estabelecidas pela lei, funcionando não apenas como um direito autônomo, mas como elemento essencial para a efetivação de outros direitos fundamentais. A caracterização da LGPD como um microssistema jurídico, com fundamentos e princípios próprios, é essencial para

contextualizar adequadamente o alcance e as implicações do direito à explicação no tratamento automatizado de dados pessoais.

5.4.1 O Microssistema da LGPD: Fundamentos, Princípios e Estrutura

O cenário global de proteção de dados pessoais foi significativamente transformado com a entrada em vigor do GDPR, estabelecendo novos padrões internacionais para o tratamento de dados pessoais. No contexto brasileiro, essa influência materializou-se na LGPD, Lei n. 13.709/2018, que incorporou diversos elementos do modelo europeu, adaptando-os à realidade nacional.

No contexto brasileiro, a LGPD emerge como um marco regulatório fundamental, estabelecendo um microssistema[60] abrangente de proteção de dados pessoais, alinhado com princípios constitucionais e voltado à proteção da dignidade e da autonomia informativa dos titulares. Este alinhamento com o GDPR não se limita apenas à estrutura normativa, mas estende-se também à interpretação e aplicação da lei, com as decisões das autoridades europeias de proteção de dados e as orientações do Comitê Europeu para a Proteção de Dados servindo como importantes referências interpretativas.

A legislação brasileira tem como objetivo principal "proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural"[61]. Seus 65 artigos disciplinam o tratamento de dados pessoais em meios digitais e físicos, tanto por pessoas naturais quanto por pessoas jurídicas de direito público ou privado. Assim, "proteger os dados pessoais e de reforçar a autonomia informativa e a dignidade dos titulares dos dados, bem como a própria democracia", permitindo a sua compatibilização "com as demais normas infraconstitucionais e ser interpretada à luz da Constituição da República" (BRASIL, 2018; SARMENTO, 2008; FRAZÃO, 2021, p. 35; LIMA, SÁ, 2020, p. 229).

Para alcançar estes objetivos fundamentais, a lei estabelece um conjunto estruturado de princípios que devem ser observados no tratamento de dados pessoais, incluindo finalidade,

[60] A LGPD é considerada um microssistema protetivo visto que "o surgimento de microssistema se verifica em razão da instalação de nova ordem protetiva sobre determinado assunto, com princípios próprios, doutrina e jurisprudência próprias, autônomos ao Direito Comum" (SÁ, 2023, p. 837).

[61] 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. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios (BRASIL, 2018).

adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (BRASIL, 2018).

Para garantir a efetiva aplicação destes princípios e demais disposições normativas, a criação da ANPD representa um elemento pilar do sistema, sendo responsável pela fiscalização e aplicação da lei. Esta estrutura institucional é fundamental para garantir a efetiva implementação das disposições legais e a proteção dos direitos dos titulares de dados (BRASIL, 2018).

Além de sua estrutura institucional robusta, a LGPD caracteriza-se por sua transversalidade, permeando "todos os setores da sociedade", desde a academia até o setor público, passando por instituições financeiras e organizações do terceiro setor. Esta abrangência reflete a compreensão de que a proteção de dados pessoais é um direito que transcende setores específicos (GOMES, 2019).

Neste contexto de aplicação abrangente, um aspecto fundamental da lei é o reconhecimento explícito da titularidade dos dados pela pessoa natural[62][63]. Esta mudança de paradigma é significativa, pois altera a perspectiva anteriormente dominante no mercado, onde os dados eram tratados como ativos próprios das empresas que os coletavam. Agora, estabelece-se claramente que os dados continuam pertencendo às pessoas às quais se referem, impondo aos agentes de tratamento um dever de prestação de contas sobre sua utilização, "conferindo-lhe extensa miríade de direitos para empreender efetivo controle sobre as suas informações" (FRAZÃO, 2019, p. 693).

Essa transformação é bem explicada por Frazão, que esclarece:

> O mercado tratava os dados coletados como ativo próprio, que poderia ser livremente utilizado e comercializado por quem deles se apropriasse. Agora a perspectiva é inversa: os dados coletados continuam a pertencer às pessoas às quais se referem, de modo que o coletor dos dados deve prestar contas do uso que deles é feito. As prerrogativas, direitos e princípios contidos na LGPD se reconduzem a essa ideia básica: dever de prestar contas, já que o agente de tratamento de dados lida com bens alheios e de extrema relevância. Esse dever fundamentalmente é gratuito e envolve também a obrigação de retificar informações para que os dados reflitam a realidade e não obstem o exercício de direitos fundamentais da pessoa natural (FRAZÃO, 2019, p. 694).

Apesar desta forte proteção aos direitos dos titulares, é importante ressaltar que a LGPD não visa obstaculizar as atividades empresariais que necessitam da coleta e processamento de

[62] Art. 5º. "Para os fins desta Lei, considera-se: [...] I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018).
[63] A norma o reconhece como titular de dados em seu art. 5º, inciso V.

dados. Pelo contrário, a lei reconhece a legitimidade do interesse em conhecer consumidores, empregados e candidatos a emprego. No entanto, esclarece que os dados coletados para uma "finalidade legítima pertencem às pessoas físicas às quais os dados se referem e precisam ser tratados e coletados em respeito à essa relação de pertencimento" (FRAZÃO, 2019, p. 696).

Para materializar este equilíbrio entre proteção e utilização legítima dos dados, para o enquadramento legal das operações de tratamento de dados, os agentes devem justificar suas atividades com base em pelo menos uma das hipóteses legais previstas na lei. Além disso, precisam desenvolver uma estrutura organizacional compatível com os princípios e deveres estabelecidos pela legislação (BRASIL, 2018).

A compreensão dos fundamentos e da estrutura geral da LGPD, enquanto microssistema de proteção de dados pessoais, estabelece a base necessária para uma análise mais específica de como a lei aborda o perfilamento digital. Esta prática, que se tornou um dos aspectos mais controversos e desafiadores do tratamento automatizado de dados, merece especial atenção devido ao seu potencial impacto nos direitos fundamentais dos titulares. Enquanto o GDPR optou por uma regulamentação explícita e detalhada do perfilamento, a LGPD adotou uma abordagem mais flexível, que precisa ser compreendida à luz dos princípios e fundamentos anteriormente discutidos. Esta análise comparativa entre os dois marcos regulatórios revela não apenas suas diferenças de abordagem, mas também como cada sistema jurídico busca equilibrar a inovação tecnológica com a proteção dos direitos individuais no contexto do perfilamento automatizado.

5.4.2 Perfilamento de Dados Pessoais: Uma Análise Comparativa entre GDPR e LGPD sob a Perspectiva do Direito à Explicação

A perfilização (*profiling*) representa uma das dimensões mais complexas e desafiadoras no âmbito da proteção de dados pessoais. No contexto brasileiro, observa-se que este tema não recebeu o mesmo tratamento detalhado conferido pelo GDPR, apresentando lacunas significativas em sua regulamentação. Como aponta Rafael Zanatta, a norma brasileira mostra-se menos restritiva em dois aspectos fundamentais: "(i) ausência de um conceito jurídico expresso e (ii) ausência de uma norma geral proibitiva ao *profiling*, como ocorreu na União Europeia" (ZANATTA, 2019, p.20).

Esta lacuna regulatória, contudo, não significa que o tema tenha sido negligenciado durante o processo legislativo. Apesar da aparente omissão legislativa, a perfilização foi objeto de importantes debates durante o processo de elaboração da LGPD. Esta preocupação ficou

evidenciada no relatório do Deputado Orlando Silva (PCdoB/SP), responsável pelos trabalhos finais da Comissão Especial de Tratamento e Proteção de Dados Pessoais, que destacou diversos riscos associados a esta prática:

> O conhecimento de marcadores genéticos pode ajudar no desenvolvimento da medicina, mas a informação também poderia ser manipulada para encarecer ou alijar pessoas do acesso ao trabalho, planos de saúde ou outros serviços. Dados locacionais adquiridos por aplicativos de trânsito podem ser repassados para seguradoras para traçar o perfil de motoristas e permitir a oferta de produtos mais baratos, mas também poderiam ser utilizados para negar cobertura a moradores de determinadas ruas ou regiões. [...] Redes de comércio varejista, autoridades de segurança pública, partidos políticos e as mais diversas associações podem igualmente estar recebendo diversos dados do perfil de internautas, usuários de telefonia ou telespectadores, e tomando decisões que afetam diretamente as vidas dessas pessoas. Em tempos em que cada pessoa possui um rastro digital praticamente impossível de ser apagado, é certo que o uso indevido ou o vazamento dessas informações poderá causar danos irreparáveis aos indivíduos e à coletividade (SILVA, 2012).

Diante destes riscos evidenciados no processo legislativo, a doutrina jurídica brasileira tem se debruçado sobre a necessidade de estabelecer garantias efetivas aos titulares de dados. Nesta linha, Bruno Bioni enfatiza que, nos casos de perfilização, a relação comunicativa deve transcender a mera notificação. Estabelece-se, assim, um processo dialógico que deve assegurar a efetiva compreensão por parte do indivíduo submetido à catalogação e análise de dados inferenciais (BIONI, 2019).

Esta perspectiva dialógica na proteção de dados não é uma inovação isolada, mas encontra fundamentação teórica robusta em outras áreas do conhecimento. Particularmente relevante é a compreensão da natureza dialógica da comunicação encontra respaldo na teoria pedagógica de Paulo Freire, que rejeita o simples "depósito de informação" em favor de um processo de construção conjunta do conhecimento. Esta abordagem é particularmente relevante no contexto da perfilização, onde a complexidade técnica dos processos demanda um esforço especial de comunicação e engajamento (FREIRE, 2002).

Como obrigação dialógica deve-se compreender que não se trata de uma comunicação unilateral, “como o envio de um relatório descritivo das fórmulas matemáticas utilizadas pelo controlador e as técnicas de estatísticas que permitem a inferência sobre um comportamento futuro a partir de um conjunto de dados pessoais e metadados” (ZANATTA, 2019, p. 22).

A partir desta compreensão sobre a natureza da obrigação dialógica, é possível identificar um conjunto mais amplo de deveres que recaem sobre os controladores de dados. Neste sentido, Rafael Zanatta defende que a perfilização e o poder de inferir alguma informação sobre o titular implica em obrigações de três naturezas: a primeira é informacional, e se

relaciona com a cientificação da existência do perfil e garantir a transparência. Em segundo ponto, ser antidiscriminatória, possui relação com as formas de utilização dos dados como raça, gênero e orientação religiosa, como determinantes na construção do perfil, e por terceiro dialógica, possui acesso à obrigação de engajar em um processo dialógico com os titulares, "garantindo a explicação de como a perfilização funciona, sua importância para determinados fins e de como decisões são tomadas." (ZANATTA, 2019, p. 22).

Dentre estas três dimensões de obrigações, merece especial atenção o aspecto da explicabilidade, que se desdobra da natureza dialógica anteriormente mencionada. Esta obrigação assume particular relevância no contexto da perfilização, uma vez que afeta diretamente as esferas pessoal e patrimonial dos titulares dos dados. Esta comunicação deve ser estruturada de forma a possibilitar o entendimento claro dos mecanismos utilizados no processamento das informações, permitindo que o titular compreenda não apenas quais dados são coletados, mas também como são interpretados e utilizados para gerar inferências sobre seu comportamento e características.

Esta necessidade de estruturação adequada da comunicação não representa, contudo, um obstáculo intransponível para as organizações. Pelo contrário, evidencia a necessidade de uma interpretação sistemática e teleológica do ordenamento jurídico, que considere tanto os princípios estabelecidos na LGPD quanto as experiências internacionais, como o GDPR, para assegurar uma proteção efetiva dos direitos dos titulares de dados em face das crescentes possibilidades de tratamento automatizado de informações pessoais. Diante deste cenário, torna-se especialmente relevante a análise do direito à explicação no contexto da LGPD, como mecanismo fundamental para garantir a transparência e a *accountability* no tratamento de dados pessoais.

A metodologia adota uma abordagem qualitativa e comparativa, fundamentada na análise documental e revisão bibliográfica especializada, com foco particular no estudo da LGPD e do GDPR, bem como na doutrina e jurisprudência pertinentes. O método comparativo estrutura-se em três níveis de análise, sendo, normativo-conceitual, examinando as definições e conceitos relacionados ao direito à explicação e à proteção de dados em cada legislação; funcional-sistemático, investigando como cada marco regulatório operacionaliza a proteção dos direitos dos titulares no contexto das decisões automatizadas; e teleológico-aplicativo, analisando as finalidades e objetivos pretendidos por cada legislação, bem como suas implicações práticas.

Esta abordagem multinível permite identificar não apenas as semelhanças e diferenças entre os marcos regulatórios, mas também compreender como cada sistema jurídico responde

aos desafios das decisões automatizadas considerando suas particularidades culturais, sociais e econômicas. A comparação é realizada a partir de categorias analíticas específicas: direito à explicação, direito à revisão, escopo de aplicação, obrigações dos controladores e mecanismos de transparência e *accountability*.

O estudo considera ainda a interpretação doutrinária e as orientações dos órgãos reguladores, especialmente a ANPD e o GTA29, buscando uma compreensão contextualizada do tratamento jurídico da explicabilidade em sistemas automatizados. A análise jurisprudencial, com destaque para o caso paradigmático do STJ sobre sistemas de *credit scoring* (REsp nº 1.419.697/RS), complementa a metodologia, permitindo compreender como os tribunais têm interpretado e aplicado os princípios de transparência algorítmica.

O perfilamento, que envolve a utilização de dados pessoais para criar perfis individuais, é um aspecto abordado pelo GDPR. A legislação estabelece um conjunto de direitos para os titulares dos dados e obrigações para os responsáveis pelo tratamento desses dados. Para compreender a aplicabilidade desta legislação no contexto do perfilamento, é fundamental identificar dois atores principais: o titular dos dados e o controlador dos dados (BIONI, 2019).

O regulamento identifica o titular de dados como a pessoa natural à qual se referem os dados pessoais, sendo estes definidos como informações que permitem a identificação direta ou indireta do indivíduo, podendo incluir identificadores digitais, dados de localização, ou aspectos relacionados à identidade física, fisiológica, genética, econômica, cultural ou social do indivíduo[64], é uma definição abrangente que reflete a complexidade e a diversidade dos dados pessoais na era digital (UNIÃO EUROPÉIA, 2018).

Por outro lado, o controlador[65] é definido como a entidade, seja pessoa física ou jurídica, pública ou privada, que determina as finalidades e os meios do tratamento de dados pessoais, agindo individualmente ou em conjunto com outros. A conceituação atribui uma responsabilidade significativa ao controlador no processo de perfilamento.

---

[64] Artigo 4º. (1) RGPD (GDPR). «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (UNIÃO EUROPÉIA, 2018).

[65] Artigo 4º (7) RGPD (GDPR). «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro (UNIÃO EUROPÉIA, 2018).

O artigo 4(4) do GDPR[66] oferece uma definição específica de perfilamento, descrevendo-o como um processo automatizado de tratamento de dados pessoais que visa avaliar aspectos particulares de uma pessoa natural. Este processo pode incluir a análise ou previsão de elementos como desempenho profissional, situação econômica, saúde, preferências pessoais, interesses, confiabilidade, comportamento e localização. Para se enquadrar na definição do GDPR, o perfilamento deve envolver três elementos essenciais: (1) um processo automatizado de tratamento, (2) o uso de dados pessoais, e (3) o objetivo de avaliar aspectos pessoais de um indivíduo (UNIÃO EUROPÉIA, 2018).

É relevante contrastar a definição de perfilamento do GDPR com outras conceituações acadêmicas, em particular a proposta por Mireille Hildebrandt, que oferece uma perspectiva mais abrangente do fenômeno. Para a autora, o perfilamento pode ser descrito como um "processo que busca identificar correlações para representar objetos humanos ou não-humanos, sejam eles individuais ou coletivos'". Esta definição supera a visão antropocêntrica e individualista do GDPR, que foca exclusivamente em pessoas naturais identificáveis, ao contemplar também entidades não-humanas e considerar tanto perspectivas individuais quanto coletivas. Na perspectiva da aplicação, Hildebrandt sugere que o perfilamento visa individualizar ou categorizar uma pessoa ou grupo, com o objetivo de avaliar riscos e oportunidades para o controlador. Esta abordagem mais ampla é particularmente relevante no contexto atual, onde a IA e o aprendizado de máquina estão cada vez mais envolvidos nos processos de tomada de decisão. Dada sua maior abrangência e aplicabilidade ao cenário tecnológico contemporâneo, este trabalho adotará o conceito proposto por Hildebrandt como referência teórica principal (HILDEBRANDT, 2008, p. 19-20).

Assim, o GTA 29[67], um órgão consultivo independente da UE sobre proteção de dados, oferece orientações adicionais sobre o perfilamento. De acordo com este órgão, o perfilamento

[66] Artigo 4 (4) RGPD (GDPR). «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações (UNIÃO EUROPÉIA, 2018).

[67] A Diretiva 95/46 da União Europeia estabeleceu um órgão consultivo denominado Grupo de Trabalho do Artigo 29. Este grupo, formado por representantes de todos os Estados Membros da UE, desempenhava um papel fundamental na interpretação e aplicação da diretiva de proteção de dados. Suas responsabilidades incluíam o fornecimento de suporte técnico, a elaboração de recomendações sobre a diretiva e a emissão de pareceres sobre práticas que pudessem impactar os direitos de proteção de dados dos cidadãos europeus. A implementação do Regulamento Geral sobre a Proteção de Dados (GDPR) em 25 de maio de 2018 marcou uma transição significativa na estrutura de governança de proteção de dados da UE. Com a entrada em vigor do GDPR, o Grupo de Trabalho do Artigo 29 foi sucedido por uma nova entidade: o Comitê Europeu para a Proteção de Dados (CEPD), também conhecido pela sigla em inglês EDPB (European Data Protection Board). Esta mudança refletiu a evolução do cenário regulatório de proteção de dados na União Europeia, com o CEPD assumindo e

não se limita apenas à previsão de comportamentos, mas engloba todo o processo de coleta e análise de dados para criar perfis, independentemente de seu uso posterior para fins preditivos.

O processo de perfilamento, conforme delineado pelo GTA29, envolve uma série de etapas sistemáticas e interligadas. A primeira etapa consiste na coleta metódica de informações sobre indivíduos ou grupos, abrangendo desde dados demográficos básicas, até padrões de comportamento complexos e preferências de consumo. Em seguida, estas informações são submetidas a uma análise aprofundada, utilizando técnicas avançadas de processamento de dados e algoritmos especializados (GRUPO DE TRABALHO DO ARTIGO 29, 2016, p. 7).

O objetivo primordial deste procedimento é identificar características distintas, padrões comportamentais ou tendências que permitam categorizar os sujeitos em grupos distintos. Esta categorização pode ser baseada em diversos critérios, como perfil de risco, potencial de consumo, ou até mesmo predisposições políticas ou ideológicas. O GTA29 enfatiza que estas análises podem ser utilizadas tanto para compreender comportamentos atuais quanto para realizar previsões sobre diversos aspectos relacionados aos indivíduos ou grupos perfilados, como a capacidades para executar determinadas tarefas, relevante em contextos de emprego ou educação; ou preferências e interesses pessoais, primordiais para estratégias de marketing personalizado.

É importante ressaltar que a definição de perfilamento proposta pelo GTA29 abrange tanto a análise individual quanto coletiva. Isto reconhece que os perfis podem ser construídos e aplicados em diferentes escalas, dependendo do objetivo e do contexto da análise. Por exemplo, um perfil pode ser criado para um indivíduo específico para fins de avaliação de crédito, ou para um grupo demográfico inteiro para estratégias de marketing em larga escala.

A análise do tratamento do perfilamento no GDPR, com sua abordagem detalhada e explícita, serve como importante referência para compreender como diferentes jurisdições abordam este desafio regulatório. Particularmente relevante é examinar como o Brasil, ao desenvolver sua própria legislação de proteção de dados, incorporou e adaptou alguns destes conceitos à realidade nacional. Embora a LGPD tenha se inspirado em diversos aspectos do modelo europeu, sua abordagem ao perfilamento apresenta características próprias que refletem as especificidades do contexto brasileiro e demonstram uma flexibilidade potencialmente vantajosa diante das rápidas transformações tecnológicas. Esta adaptação do modelo europeu à realidade brasileira merece uma análise detalhada, principalmente considerando como as

expandindo as funções anteriormente desempenhadas pelo Grupo de Trabalho do Artigo 29, adaptando-se às novas exigências e desafios apresentados pelo GDPR (EUROPA, 2024).

diferentes abordagens regulatórias podem impactar a proteção efetiva dos direitos dos titulares de dados.

Após compreender como o GDPR aborda o perfilamento no contexto europeu, é fundamental analisar como esta prática é tratada na legislação brasileira. A LGPD, inspirada em diversos aspectos pelo regulamento europeu, apresenta suas próprias particularidades no tratamento desta questão. Embora ambas as legislações compartilhem princípios fundamentais de proteção de dados e privacidade, suas abordagens quanto ao perfilamento revelam diferenças significativas que refletem as especificidades de seus respectivos contextos jurídicos e sociais.

Neste sentido, a norma brasileira delimita os conceitos a serem aplicados ao microssistema de proteção de dados em seu artigo 5º. De forma análoga ao GDPR, a norma brasileira apresenta definições claras para "titular de dados"[68] e "controlador de dados"[69]. O titular de dados é definido como "a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento", enquanto o controlador é definido como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (BRASIL, 2018).

Contudo, diferentemente do GDPR, a LGPD não apresenta uma definição explícita do conceito de perfilamento. Em vez disso, a lei brasileira utiliza o termo “perfil” em contextos específicos. Uma menção notável ocorre no artigo 12, § 2º da LGPD[70], que trata da anonimização de dados. Este dispositivo estabelece uma exceção à regra geral, indicando que dados pessoais anonimizados, quando utilizados para fins de formação de perfil comportamental de pessoa natural identificada, serão considerados como dados pessoais.

Esta abordagem da LGPD confere à norma um caráter protetivo, alinhado com o princípio fundamental de proteger os titulares de dados dos potenciais consequências adversas do tratamento de dados pessoais. Como observa Bruno Bioni, o intuito é “proteger os titulares de dados das consequências que o tratamento de dados pessoais pode ter em sua esfera individual e em seu livre desenvolvimento” da personalidade. O caráter protetivo da LGPD é evidenciado pela sua preocupação com os efeitos do tratamento de dados sobre os indivíduos, indo além da mera identificação pessoal (BIONI, 2019, p.80).

---

[68] Art. 5º. [...] V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (BRASIL, 2018).

[69] Art. 5ª. [...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (BRASIL, 2018).

[70] Art. 12. [...] § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (BRASIL,2018).

A ausência de uma definição explícita de perfilamento na LGPD não implica em uma falta de proteção contra práticas potencialmente abusivas. Pelo contrário, a lei brasileira adota uma abordagem mais flexível e adaptável, que pode ser interpretada de forma a abranger uma ampla gama de práticas de perfilamento, à medida que estas evoluem com o avanço tecnológico.

A interpretação do art. 12, § 2º, que menciona "determinada pessoa" e "identificada", deve ser realizada de forma ampla, considerando não apenas a atribuição de um perfil comportamental específico, mas também os impactos que o tratamento de dados pode ter sobre o indivíduo. Esta visão está em consonância com a abordagem holística da lei, que engloba tanto pessoas identificadas quanto identificáveis, reforçando o princípio do livre desenvolvimento da personalidade, como expresso nos artigos 1º[71] e 2º, VII[72] (BIONI, 2019).

O artigo 20[73] da LGPD aborda especificamente o direito à revisão e explicação de decisões automatizadas, aplicando-se a situações em que tais decisões baseadas exclusivamente em processamento automatizado afetam os interesses dos titulares dos dados. É um dispositivo é particularmente relevante no contexto do perfilamento, pois inclui as decisões que visam definir perfis pessoais, profissionais, de consumo e de crédito, ou aspectos da personalidade do indivíduo.

Cabe ainda mencionar que o art. 4º, III[74], da LGPD restringe sua aplicação em casos de tratamento de dados para fins exclusivos para segurança pública, defesa nacional e repressão das infrações penais. A limitação foi imposta para garantir o interesse público de combater as infrações penais, crime organizado, fraudes ou terrorismo (BRASIL, 2018).

Contudo, está limitação não é absoluta. O parágrafo primeiro do mesmo artigo[75] estabelece que os princípios gerais de proteção devem nortear qualquer esfera de tratamento, inclusive em contextos de interesse público. Isso significa que princípios fundamentais como transparência, finalidade, adequação, necessidade, livre acesso, qualidade dos dados e

---

[71] 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 (BRASIL,2018).

[72] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL,2018).

[73] Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (BRASIL,2018).

[74] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: [...] III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais (BRASIL,2018).

[75] Art. 4º. [...] § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei (BRASIL,2018).

segurança (art. 6º[76], 17[77] e 18[78] da LGPD) continuam sendo garantias essenciais dos direitos dos titulares de dados, mesmo nessas situações específicas (BRASIL,2018).

A LGPD não vincula explicitamente o perfilamento a processos automatizados, nem especifica finalidades restritas para a criação de perfis. Esta perspectiva mais ampla permite uma interpretação mais abrangente das práticas de perfilamento, potencialmente englobando uma gama maior de aplicações e contextos de tratamento de dados pessoais no Brasil (MENDES, 2020).

A flexibilidade da LGPD em relação ao perfilamento pode ser vista como uma vantagem, pois possibilita que a lei se adapte a novas tecnologias e práticas de tratamento de dados que possam emergir no futuro. No entanto, essa abordagem também exige uma interpretação cuidadosa e contextualizada da lei por parte dos operadores do direito e dos agentes de tratamento de dados, para garantir que a proteção dos titulares seja efetiva em diferentes cenários.

A perspectiva mais ampla sobre o perfilamento oferecida pela LGPD pode ter implicações significativas na interpretação e aplicação da lei em diversos contextos de tratamento de dados pessoais no Brasil. Isso permite uma adaptabilidade maior às particularidades do cenário brasileiro e às rápidas mudanças tecnológicas, mas também requer uma vigilância constante para garantir que essa flexibilidade não resulte em brechas que possam comprometer a proteção dos dados pessoais.

Embora ambas as normas estabeleçam salvaguardas e proteções, que objetivam a transparência na utilização dos dados de entrada que serão utilizados para a formação dos perfis, há uma notável escassez de informações detalhadas sobre os métodos utilizados para chegar a

---

[76] Art. 6º. As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (i) confirmação da existência de tratamento; (ii) acesso aos dados; (iii) correção de dados; (iv) anonimização, bloqueio ou eliminação de dados desatualizados, excessivos ou tratados em desconformidade com a lei; (v) portabilidade de dados; (vi) eliminação dos dados pessoais tratados com o consentimento, (vii) informações sobre o compartilhamento de dados; (viii) informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; (ix) revogação do consentimento (BRASIL,2018).

[77] Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei (BRASIL,2018).

[78] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei (BRASIL,2018).

essas inferências, representando um desafio significativo no que diz respeito à transparência efetiva.

Esta lacuna informacional obscurece aspectos importantes do processo de perfilamento, tais como os tipos específicos de dados utilizados na construção de perfis, o peso atribuído a cada elemento de dados e, crucialmente, como esses fatores influenciam a categorização dos indivíduos em diferentes perfis. A opacidade desses processos não apenas dificulta a compreensão por parte dos titulares de dados, mas também pode comprometer a eficácia das proteções legais estabelecidas.

Diante dessa problemática, Sandra Wachter e Brent Mittelstadt propõem uma abordagem mais rigorosa e protetiva. Os autores sugerem que certas inferências, particularmente aquelas classificadas como de "alto risco", deveriam ser tratadas com o mesmo nível de proteção que os dados pessoais. Estas inferências de alto risco podem incluir aquelas que têm o potencial de causar danos reputacionais, invadir a privacidade do indivíduo, ou que são utilizadas para fundamentar decisões importantes sem possibilidade de verificação. A justificativa para esta proposta é proporcionar aos titulares dos dados uma maior visibilidade sobre as inferências feitas a seu respeito (WACHTER; MITTELSTADT, 2019).

A implementação de mecanismos mais robustos de transparência e prestação de contas no processo de perfilamento, além de aumentar a confiança dos titulares de dados, tem o potencial de promover práticas mais éticas e responsáveis por parte das organizações envolvidas no tratamento de dados pessoais. Esta orientação alinharia a prática brasileira com as tendências globais de proteção de dados, mantendo simultaneamente a flexibilidade necessária para adaptar-se às particularidades do contexto nacional e às rápidas evoluções tecnológicas.

Neste contexto de busca por maior transparência e prestação de contas, emerge um elemento fundamental para a efetividade do perfilamento ético e responsável: a explicabilidade. Este conceito transcende a mera disponibilização de informações sobre o processo de perfilamento, estabelecendo-se como um requisito essencial para garantir que as decisões baseadas em perfis sejam compreensíveis e justificáveis. A explicabilidade atua como ponte entre a complexidade técnica dos sistemas de perfilamento e a necessidade de compreensão por parte dos titulares de dados, possibilitando não apenas o entendimento dos processos, mas também o exercício efetivo dos direitos previstos tanto na LGPD quanto no GDPR.

A explicabilidade, um tema de crescente relevância no campo da proteção de dados e da IA, confere a capacidade de fornecer explicações claras e compreensíveis sobre como as inferências são realizadas e como as decisões baseadas em perfis são tomadas é fundamental

para garantir a efetividade das proteções legais e o exercício pleno dos direitos dos titulares de dados.

O aprofundamento no conceito de explicabilidade permite uma compreensão mais ampla dos desafios e possíveis soluções para aumentar a transparência e a *accountability* nos processos de perfilamento. Isso contribui para um uso mais ético e responsável dos dados pessoais em uma era cada vez mais dominada por algoritmos e IA. A explicabilidade não só fortalece a confiança dos usuários, mas também facilita a identificação e correção de vieses algorítmicos, promovendo assim uma maior equidade no tratamento de dados.

No contexto da LGPD, a explicabilidade ganha ainda mais relevância quando consideramos o direito à revisão de decisões automatizadas, previsto no artigo 20 da lei. Este dispositivo legal exige que os titulares de dados tenham acesso a informações claras e adequadas sobre os critérios e procedimentos utilizados para a decisão automatizada. A implementação efetiva deste direito depende diretamente da capacidade dos sistemas de IA de fornecerem explicações compreensíveis sobre seus processos decisórios (BRASIL, 2018).

A busca por maior transparência e explicabilidade nos sistemas de IA não é apenas uma questão técnica, mas também um imperativo ético e legal. À medida que a IA se torna mais ubíqua e influente em diversos aspectos da vida social e econômica, a necessidade de compreender e regular seus impactos torna-se cada vez mais premente. Isso demanda uma abordagem interdisciplinar, que combine conhecimentos de ciência da computação, direito, ética e ciências sociais.

A análise do perfilamento no contexto das legislações de proteção de dados, especialmente na comparação entre GDPR e LGPD, revela uma preocupação crescente com a transparência e a explicabilidade dos processos automatizados de tratamento de dados pessoais. Essa preocupação se materializa de forma mais concreta no direito à explicação, um elemento fundamental para garantir que os titulares de dados possam compreender e questionar as decisões que os afetam. No ordenamento jurídico brasileiro, o direito à explicação emerge como uma garantia essencial, especialmente considerando que o artigo 20 da LGPD estabelece o direito à revisão de decisões automatizadas. Este dispositivo, embora não use expressamente o termo "direito à explicação", estabelece as bases para uma interpretação que privilegia a transparência e a compreensibilidade dos processos decisórios automatizados. Compreender como esse direito se estrutura e se manifesta no contexto brasileiro é fundamental para avaliar a efetividade da proteção dos titulares de dados em um cenário de crescente automatização e uso de inteligência artificial (BRASIL, 2018).

5.4.3 O Direito à Explicação no Contexto das Decisões Automatizadas

O artigo 20 da LGPD estabelece garantias fundamentais aos titulares de dados em relação às decisões automatizadas, conforme disposto em seu texto:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
> § 1º. O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º. Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (BRASIL, 2018).

A legislação estabelece no caput do artigo 20 que o titular de dados pessoais possui "o direito a solicitar a revisão de decisões tomadas **unicamente** com base em tratamento automatizado de dados pessoais, desde que afetem seus interesses" (BRASIL, 2018, grifo nosso).

Adicionalmente, o § 1º determina a obrigatoriedade do controlador em fornecer informações claras e adequadas sobre os critérios e procedimentos utilizados na decisão automatizada, respeitando os segredos comercial e industrial (BRASIL, 2018).

No contexto do tratamento automatizado, o titular possui um conjunto de direitos específicos, incluindo, a solicitação de revisão (art. 20, caput); o acesso a informações sobre critérios e procedimentos utilizados (art. 20, § 1º); a possibilidade de solicitar à ANPD uma auditoria para verificar aspectos discriminatórios, caso o controlador negue informações alegando segredo comercial e industrial (art. 20, § 2º c/c art. 18 § 1º); o direito de oposição ao tratamento (art. 18, § 2º); e o direito de oposição à decisão automatizada (art. 18, §2º).(BRASIL, 2018).

O escopo de aplicação da lei contempla decisões tomadas exclusivamente por sistemas automatizados que afetam interesses dos titulares, definem perfis pessoais, profissionais, de consumo ou crédito e impactam aspectos da personalidade. Uma questão relevante na análise desta norma é a ausência de uma definição precisa do termo "decisões automatizadas". Para suprir esta lacuna, o Projeto de Lei nº 4496/19, proposto pelo Senador Styvenson Valentim (PODEMOS/RN), sugere a inclusão do inciso XX ao artigo 5º da LGPD, que define decisão automatizada como um processo de escolha, classificação, aprovação ou rejeição, atribuição de nota, medida, pontuação ou escore, cálculo de risco ou probabilidade, realizado através do

tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, IA, aprendizado de máquina ou outra técnica computacional:

> XX – decisão automatizada: processo de escolha, de classificação, de aprovação ou rejeição, de atribuição de nota, medida, pontuação ou escore, de cálculo de risco ou de probabilidade, ou outro semelhante, realizado pelo tratamento de dados pessoais utilizando regras, cálculos, instruções, algoritmos, análises estatísticas, IA, aprendizado de máquina, ou outra técnica computacional (BRASIL, 2019).

Embora o art. 20 da LGPD não seja explícito quanto à sua aplicação nas decisões tomadas por IA, no contexto atual de hipertecnologias[79], é impossível ignorar o início da regulamentação de seu uso. O conceito apresentado pela proposta legislativa demonstra a abrangência da "amplitude da expressão, que não se limita aos casos de decisão por sistemas de IA" (BIONI, LUCIANO; 2019; LIMA, SÁ, 2020, p. 231).

Para uma compreensão mais aprofundada do impacto desta regulamentação nas decisões automatizadas, é necessário estabelecer uma distinção fundamental entre algoritmos convencionais e sistemas de IA. Thatiane Cristina Pires e Rafael Petelfi da Silva enfatizam que a IA é caracterizada pelo processo de raciocínio, motivação e comportamento:

> Pra definir a IA, Russel e Norving identificam duas principais características: uma associada como processo de raciocínio e motivação, e outra ligada ao comportamento. Nesse sentido, a principal diferença entre um algoritmo convencional e a IA está, justamente, na habilidade de acumular experiências próprias e extrair delas aprendizado, como um autodidata. Esse aprendizado, denominado de machine learning, permite à IA atuar de forma diferente em uma mesma situação, a depender da sua performance anterior – o que é muito similar à experiência humana (PIRES; SILVA, 2017, p.239).

O texto original do artigo 20 da LGPD previa que a revisão fosse realizada por "pessoa natural", em consonância com o GDPR. Esta disposição foi posteriormente alterada pela Medida Provisória nº 869/2018, convertida na Lei nº 13.853/19. A justificativa apresentada pelo então Presidente Jair Bolsonaro para esta modificação baseou-se no argumento de que a exigência de revisão humana para todas as decisões automatizadas poderia comprometer modelos de negócios existentes, particularmente de startups e instituições financeiras, com potencial impacto na oferta de crédito e na economia:

---

[79] O conceito de hipertecnologias refere-se ao uso avançado e integrado de tecnologias que vão além das capacidades tradicionais, combinando IA, big data, internet das coisas (IoT), blockchain, realidade aumentada (AR) e realidade virtual (VR), entre outras. Estas tecnologias não apenas se destacam por suas funcionalidades isoladas, mas, sobretudo, pela forma como se interconectam e se potencializam mutuamente, criando soluções inovadoras e disruptivas para uma ampla gama de setores.

> A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária (BRASIL, 2018).

A supressão do termo "pessoa natural" do texto original do artigo 20 da LGPD, em contraste com a abordagem do GDPR, suscita diversas interpretações sobre os procedimentos de revisão de decisões automatizadas no contexto brasileiro. Esta ambiguidade legislativa evidencia a necessidade de um debate continuado sobre a regulamentação da IA e a proteção dos direitos dos titulares de dados pessoais no Brasil (BRASIL, 2018).

Para melhor visualizar estas diferenças regulatórias e suas implicações práticas segue um quadro comparativo:

Aspecto	GDPR (Regulamento Geral de Proteção de Dados da União Europeia)	LGPD (Lei Geral de Proteção de Dados do Brasil)
Base Legal	Artigo 22	Artigo 20
Direito Básico	O titular tem o direito de não se sujeitar a decisões automatizadas.	O titular tem o direito de solicitar a revisão de decisões automatizadas.
Interferência Humana	Garante o direito de obter intervenção humana, manifestar seu ponto de vista e contestar a decisão.	Garante o direito de solicitar revisão de decisão automatizada por pessoa natural.
Afetação dos Interesses	As decisões automatizadas não devem produzir efeitos jurídicos ou afetar significativamente o titular.	As decisões automatizadas não devem afetar os interesses dos titulares de forma significativa.
Exceções	- Necessidade para execução de contrato. - Autorização pela legislação da União ou do Estado-Membro. - Consentimento explícito do titular.	- Necessidade para execução de contrato. - Cumprimento de obrigação legal. - Exercício regular de direitos em processo judicial, administrativo ou arbitral.
Medidas Adequadas	Exige medidas adequadas para salvaguardar direitos, liberdades e interesses legítimos.	Exige medidas para proteger direitos e garantias do titular, incluindo a revisão de decisões automatizadas.
Perfilamento	Inclui a definição de perfis como parte das decisões automatizadas.	Define explicitamente a elaboração de perfis e suas implicações.
Categorias Especiais de Dados	Decisões baseadas em dados sensíveis são restritas e requerem proteção adicional.	Decisões baseadas em dados sensíveis são permitidas apenas com consentimento explícito ou em situações específicas previstas em lei.

Fonte: Quadro desenvolvido pela Autora.

O direito à explicação manifesta-se como uma expressão do princípio da transparência, conforme previsto expressamente no art. 6º, VI da LGPD[80]. No contexto da coleta de dados pessoais por meio de tecnologias com IA, destaca-se a relevância do acesso do indivíduo às suas próprias informações. As legislações de proteção de dados exercem função crucial na salvaguarda do direito de acesso, constituindo este "antes de tudo, um instrumento diretamente acionável pelos interessados, que podem utilizá-lo não somente como a finalidade de simples conhecimento, mas também para promover propriamente a efetividade" (BRASIL, 2018; RODOTÀ, 2008, p. 60).

Na doutrina, Laura Schertel Mendes defende que o direito à explicação constitui uma garantia autônoma, fundamentando-se na compreensão de que a LGPD estabelece um direito próprio do titular dos dados de compreender a lógica subjacente ao tratamento automatizado. Esta interpretação é corroborada por Danilo Doneda, referência fundamental em proteção de dados no Brasil, que reconhece a autonomia do direito à explicação principalmente com base no artigo 20 da LGPD, identificando características e objetivos específicos que o distinguem de outras garantias previstas na lei (MENDES, 2014; DONEDA, 2021).

Uma corrente doutrinária alternativa, representada por Renato Monteiro, compreende o direito à explicação como uma ramificação do direito de acesso, interpretando-o como uma manifestação específica desta garantia mais ampla no contexto das decisões automatizadas:

> Ao incluir 10 princípios gerais de proteção de dados pessoais, a Lei garante aos titulares dos dados o direito à transparência, ou seja, o direito de obter "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". Ou seja, a garantia para que se requisite de órgãos públicos e privados informações sobre como os seus dados são usados. Esse direito, que dá origem ao direito de acesso aos dados, é complementado pelo artigo 19, que determina que "A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular" e se darão "por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular (MONTEIRO, 2018, p.9).

Este direito é complementado pelo artigo 19, que determina que a confirmação de existência ou o acesso a dados pessoais serão providenciados mediante requisição do titular, através de declaração clara e completa.

---

[80] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (BRASIL, 2018).

Segundo Rodotà, é imperativo que seja “concedido à pessoa o poder de controle direto sobre os coletores de informações, independemente da existência de uma violação a seus direitos". Esta abordagem visa estabelecer um equilíbrio nas dinâmicas de circulação de informações, fortalecendo a posição dos indivíduos, suprindo a lacuna entre o poder entre estes e os 'senhores da informação'" (COSTA; DE OLIVEIRA; NEGRI *apud* RODOTÀ, 2013, p. 95; RODOTÀ, 2008).

O direito à explicação necessita ser compreendido como componente integrante de um sistema jurídico mais amplo, estabelecendo conexões significativas com outros princípios fundamentais, como transparência, adequação e autodeterminação informativa. A interseção entre a LGPD e o CDC estabelece um robusto arcabouço de proteção ao titular de dados nas relações de consumo, com particular ênfase na fase pré-contratual (FALEIROS; MEDON, 2021).

Nesta linha, este presente trabalho, contudo, propõe uma interpretação que reconhece a natureza híbrida[81] do direito à explicação, compreendendo-o simultaneamente como um direito autônomo e como uma espécie de responsabilidade. Esta dupla natureza reflete tanto a necessidade de garantir ao titular dos dados o poder de compreender e questionar decisões automatizadas quanto a obrigação dos controladores de dados de implementar sistemas transparentes e explicáveis.

A complexidade desta natureza híbrida e suas implicações para o ordenamento jurídico serão aprofundadas na seção subsequente, onde será examinado como a explicabilidade se manifesta como uma espécie de responsabilidade civil, analisando suas dimensões preventivas e reparatórias no contexto das decisões automatizadas. Esta análise permitirá compreender como o direito à explicação transcende a mera garantia individual para se configurar como um mecanismo essencial de governança algorítmica e *accountability*.

Este sistema de proteção encontra seu fundamento no princípio da boa-fé objetiva, que permeia todo o ordenamento jurídico brasileiro e assume relevância especial no contexto digital. A convergência normativa entre estes dispositivos legais estabelece parâmetros comportamentais que vinculam os fornecedores a um dever fundamental de proteção dos dados pessoais, especialmente no ambiente digital, onde as práticas de coleta e processamento de dados tornaram-se rotineiras (FALEIROS; MEDON, 2021).

Segundo a pesquisadora Ana Frazão, o art. 20 resulta de um conjunto de prerrogativas derivadas dos princípios estabelecidos no art. 6º, não se limitando apenas à autodeterminação

[81] Natureza híbrida é aquela que faz referência à natureza jurídica de mais de um ramo do Direito (BRASIL, 2024).

informativa prevista no art. 2º, II, da LGPD. Conclui-se que deste artigo origina-se várias salvaguardas e tutelas (FRAZÃO, 2018b; FRAJHOF, 2021).

A garantia do direito à explicação constitui uma das evidências de atuação legítima do controlador, conforme argumentam Maria de Fatima Freire de Sá e Taisa Maria Macena de Lima em sua análise sobre o direito à explicação no Brasil. As autoras destacam que:

> Neste contexto, deve ser salientado que a LGPD admite o tratamento de dados pessoais e dados sensível (nesta última categoria, incluídos os dados de saúde e dados genéticos), sem o consentimento do titular, quando houver legítimo interesse do próprio controlador ou mesmo de terceiro, inclusive nos casos de tratamento de dados realizados por sistema de IA. O direito à explicação pode tornar-se um instrumento eficiente para avaliar a legitimidade dos controladores em tais casos (SÁ; LIMA, 2020, p.235).

Neste contexto, o direito à explicação pode funcionar como instrumento eficaz para avaliar a legitimidade dos controladores.

A efetividade do direito à revisão de decisões automatizadas apresenta questionamentos quando não há intervenção humana. Observam-se desafios técnicos significativos na implementação de sistemas capazes de analisar e processar autonomamente pedidos de revisão. Esta abordagem pode, ainda, restringir a autonomia do indivíduo solicitante, que pode carecer do conhecimento específico necessário para interagir efetivamente com o sistema ou interpretar as respostas fornecidas.

A implementação desta legislação pressupõe uma série de procedimentos prévios e posteriores, integrando diferentes campos do conhecimento, como robótica e direito. Observa-se a aplicação do princípio da prevenção em conjunto com o princípio da prestação de contas[82], levando à adoção de medidas preventivas. Isso direciona a discussão sobre o direito à explicação para o conceito de *accountability* algorítmico, sendo este direito uma das formas de implementar a prestação de contas (KAMINSKI, 2016b).

Ressalta-se que, embora a lei assegure o direito de solicitar revisão, isto não implica necessariamente em alteração do resultado final após a análise do pedido. A revisão pode simplesmente confirmar a decisão original tomada pelo sistema automatizado (MULHOLLAND; FRAJHOF, 2019).

A ausência de supervisão humana direta nas tomadas de decisão automatizadas pode resultar em uma perda significativa de controle sobre esses processos. As decisões tomadas

[82] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

podem ser independentes do seu proprietário ou do programador, alcançando resultados imprevisíveis. Os sistemas que executam tarefas sem direção humana ou supervisão são denominados "autônomos", enquanto aqueles que aprendem livremente são classificados como *machine learning* (SÁ; LIMA, 2020).

Este cenário de autonomia tecnológica traz consigo desafios significativos para a proteção dos direitos dos titulares. A inexistência de uma camada de revisão humana pode potencializar problemas como vieses algorítmicos, erros de classificação e decisões injustas ou discriminatórias, sem um mecanismo eficaz para identificação e correção dessas falhas. Esta questão gerou duas principais correntes doutrinárias:

A primeira corrente, representada por Caitlin Mulholland e Isabella Frajhof, adota uma abordagem hermenêutica, sugerindo que "a alteração do texto legal importou em suprimir a possibilidade de revisão da decisão automatizada por pessoa natural". Nesta interpretação, as decisões automatizadas "seriam revisadas mediante outra decisão automatizada" (MULHOLLAND; FRAJHOF LIMA, 2019, p.266; SÁ, 2020, p. 232).

A segunda linha argumentativa sustenta que, como "as condições da revisão não estão detalhadas na LGPD", não há vedação explícita à revisão por pessoa natural. Esta interpretação permite, sem obrigar, que a revisão seja realizada por outro sistema automatizado em vez de um humano. Defensores desta visão argumentam que a "revisão por pessoa natural é mais apta a corrigir eventuais discriminações decorrentes de processo algorítmicos e dar concretude aos princípios da transparência e da responsabilidade no tratamento de dados pessoais" (LIMA, SÁ, 2020, p. 232).

Um aspecto particularmente preocupante é a opacidade dos métodos de IA, especialmente aqueles que empregam ML. Caitlin Mulholland e Isabella Frajhof alertam que a falta de transparência pode "abrir espaço para uma opacidade típica de sistemas autoritários não regulados" (MULHOLLAND; FRAJHOF, 2019, p. 272-273).

Rodotà defende "o poder incondicional que a pessoa deve ter de saber quem possui, quais dados sobre ela/ele e como esses dados são usados". O conhecimento de "quais tecnologias são empregadas, quais as práticas, como se dá o recolhimento, uso e distribuição dos seus dados" é fundamental para empoderar o cidadão no exercício de sua própria proteção (RODOTÀ, 2013, p. 109; COSTA; NEGRI; DE OLIVEIRA, 2020, p. 96).

Apesar da ausência deste requisito na norma brasileira, outras propostas consideram a supervisão humana, em qualquer fase do desenvolvimento da IA, um princípio ético ou um

elemento fundamental. Entre os exemplos incluem-se documentos elaborados pela OCDE[83], IBM e Microsoft[84], Relatório "European Group on Ethics in Science and New Technologies Artificial Intelligence, Robotics and 'Autonomous' Systems", a Estratégia Brasileira para a IA do MCTIC[85], a "The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems" e Princípios de Asilomar[86].

O artigo 20 da LGPD estabelece que o controlador deve disponibilizar ao titular todas as informações pertinentes aos critérios e procedimentos utilizados, preservando-se o segredo industrial e comercial. Esta disposição suscita importantes debates acerca da extensão e natureza das informações a serem disponibilizadas, considerando o risco de que a proteção ao segredo empresarial possa servir como subterfúgio para ocultar decisões discriminatórias ou pouco transparentes (BRASIL, 2018).

Diante desta complexa relação entre transparência e proteção do segredo empresarial, emerge uma discussão crucial sobre os meios mais adequados para garantir a explicabilidade das decisões automatizadas. A questão da explicabilidade e transparência transcende a mera disponibilização do código fonte[87], perspectiva tradicionalmente defendida por parte da doutrina. O acesso ao código fonte, embora aparentemente uma solução direta, apresenta limitações significativas, podendo comprometer a vantagem competitiva das empresas e, consequentemente, a livre concorrência. Além disso, a complexidade das estruturas de programação modernas torna o código fonte um instrumento "pouco eficaz para a compreensão dos resultados produzidos" (FERRARI; BECKER; WOLKART, 2018; NUNES; ANDRADE, 2023; VIEGAS *et. al.*; 2024, p. 16).

Neste sentido posiciona-se Burrell *apud* Isabela Ferrari:

> Como salienta Burrell, a opacidade dos learners é consequência da alta dimensionalidade de dados, da complexidade de código e da variabilidade da lógica

[83] A OCDE elaborou um documento denominado "Recommendation of the Council on Artificial Intelligence" com a finalidade de que os membros aderentes promovam e implementem medidas para promover confiança e benefícios a todas as partes interessadas (BELCHIOR, 2020).

[84] A IBM e a Microsoft assinaram um documento que denominado de "Chamada de Roma para Ética, ma espécie de juramento feito pelas empresas e o Vaticano para que tecnologias de IA sejam aprimoradas em prol da evolução humana (ARBULU, 2020).

[85] A Estratégia Brasileira de IA (EBIA) é um plano do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) que tem como objetivo promover a pesquisa e o desenvolvimento de IA no Brasil, implementado através da Portaria MCTIC nº 1.122/20 (MINISTÉRIO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO, 2020).

[86] Os Princípios de IA de Asilomar, um conjunto de diretrizes éticas para a pesquisa e desenvolvimento de IA (IA) que foram criados durante uma conferência realizada em janeiro de 2017 em Asilomar, na Califórnia. A conferência reuniu mais de 1000 especialistas em IA, incluindo pesquisadores, empresários, representantes do governo e da sociedade civil, para discutir o futuro da tecnologia e os desafios éticos e sociais associados (HAY, 2024).

[87] Denominada de transparência algorítmica.

> de tomada de decisões. Por empregarem centenas ou milhares de regras, por suas predições estarem combinadas probabilisticamente de formas complexas, pela velocidade no processamento das informações, e pela multiplicidade de variáveis operacionais, parece estar além das capacidades humanas apreender boa parte – senão todas – as estruturas decisórias que empreguem a técnica de machine learning. Assim, o mero acesso ao código comunica muito pouco, remanescendo a dificuldade de compreender o processo decisório (BURRELL *apud* FERRARI, 2019).

Nesse contexto, emerge a necessidade de desenvolver abordagens mais efetivas para garantir a compreensibilidade dos algoritmos. Isabela Ferrari, Daniel Becker e Erik Wolkart argumentam que a verdadeira compreensibilidade se manifesta quando um ser humano consegue articular a lógica subjacente a uma decisão específica, identificando a influência de determinados inputs no resultado final (FERRARI; BECKER; WOLKART, 2018).

Dierle Nunes e Otávio Andrade propõem soluções alternativas para enfrentar as diferentes formas de opacidade, enfatizando a importância da regulamentação do acesso às informações, da educação dos usuários e da implementação de processos de auditoria. Os autores ressaltam que a mera disponibilização do código e o desenvolvimento da capacidade de leitura computacional são insuficientes para assegurar a efetiva transparência do sistema, dada a complexidade e heterogeneidade das operações algorítmicas: "Regulamentação, acesso parcial ao código e a auditoria algorítmica (no caso do sigilo intencional), além dos esforços educacionais e de informação, que visam facilitar a leitura ou traduzir os códigos para o público em geral (no caso do analfabetismo técnico)" (NUNES; ANDRADE, 2023, p. 7).

Um caso emblemático que ilustra os desafios práticos da implementação desta legislação é o do Grupo Raia-Drogasil (Grupo RD). O Grupo RD foi notícia em veículos midiáticos em razão da nova política de extração de dados de seus consumidores através da ferramenta de coleta biométrica. O grupo oferecia um programa de relacionamento com o cliente no qual oferecia desconto aos consumidores que se baseava no cadastramento e fornecimento do CPF e biometria que compunha o histórico de compras (OLIVEIRA, 2022).

Quando indagados pelos consumidores as razões de tal coleta, a resposta se vinculava a requisitos de adequação da LGPD. Entretanto, quando o grupo foi questionado por órgãos com IDEC e PROCON-SP, a resposta foi pela desistência do fornecimento do cadastro biométrico. O que, por óbvio, levantou suspeitas. O caso foi apresentado em reportagem pela rede *The Intercept*[88], na reportagem intitulada, "Não cadastre sua biometria na Droga Raia – e nem em qualquer farmácia" (OLIVEIRA, 2022; DIAS, 2021, p. 1).

[88] The intercept se autointitula como uma publicação, na forma de jornal on-line independente. Foi lançada em fevereiro 2014 pela First Look Media. A organização de notícias foi criada e financiada por Pierre Omidyar, fundador da eBay, e os seus editores são Laura Poitras, cineasta, documentarista e escritora e Jeremy Scahill, jornalista investigativo norte-americano, especialista em assuntos de segurança nacional e autor do

O Grupo Raia-Drogasil chamou atenção por ser administradora de empreendimentos que fornecem diversas soluções ao mercado de saúde, são parte as marcas Raia, Drogasil e Onofre, acrescidas de outras, como, a *Univers*, que administra o grupo de benefícios de medicamentos, a *Stix*, plataforma de recompensa (troca de pontos por produtos e descontos) de grandes marcas, como a Pão de Açucar, Extra e o Banco Itaú. Além do grupo de investimentos, RD Ventures, e adquiriu em 2020 a *big tech*, *HealthBit*, que oferece serviço de IA para aprimorar o uso de planos de saúde e prevenção de casos graves em grandes empresas (OLIVEIRA, 2022).

A política de privacidade da Droga Raia previa a possibilidade de compartilhamento de informações dos consumidores entre as empresas do mesmo grupo econômico, parceiros da indústria farmacêutica, consultorias, empresas de tecnologias parceiras, sem transparecer quais dados eram compartilhados, quais as empresas compunham o mesmo grupo econômico e quais são as empresas de tecnologia parceiras (DROGA RAIA, 2020)

As empresas não declararam qual a finalidade dos dados coletados, tão pouco como foram tratados, mas hipóteses surgiram, para o IDEC é possível que a coleta tenha ocorrido para a pratica de seleção adversa, que constitui "quando o agente/principal tem informações sobre suas características individuais que lhe permitem agir de maneira oportunista já antes de um estabelecimento de contrato". Ou seja, na pratica, no instante de transação econômica, a farmácia conhece profundamente o consumidor, induz ou altera a compra com base no histórico do cliente (STANCIOLI, 2002).

Para a Intercept, permite a transferência de dados para empresas de recrutamento e seleção, utilizando como exemplo a situação em que o consumidor adquire frequentemente omeprazol. Nesse contexto, a empresa sugere que o consumidor pode estar enfrentando um problema sério de saúde no estômago ou sofrendo de gastrite nervosa. Essas informações são consideradas relevantes para os departamentos de Recursos Humanos, que buscam reduzir custos com internações, embora o indivíduo possa preferir não divulgar seu estado de saúde ao empregador (DIAS, 2021).

Uma das consequências é a alteração da finalidade do tratamento de dados, por exemplo, exames realizados para checagem da saúde, possam ser utilizados para definir o fato preditivo para contratação de plano de saúde. É um cenário que novos usos em um contexto diverso podem gerar novas e inesperadas informações sobre um grupo de pessoas ou sobre uma pessoa. Cenário que ameaçam direitos fundamentais como a liberdade, livre desenvolvimento da

livro *Blackwater: The Rise of the World's Most Powerful Mercenary Army* A versão brasileira entrou no ar dia 2 de agosto de 2016

pessoa, privacidade, autonomia, igualdade, privacidade e proteção de dados, bem como aos fundamentos do Estado Democrático de Direito.

Com a aquisição de uma empresa desenvolvedora de IA, é possível antecipar que os dados coletados poderão ser utilizados para alimentar sistemas automatizados de análise e decisão.

Assim, os agentes de tratamento devem adotar "posturas de conformidade e adesão a parâmetros regulatórios que aclarem a interseção entre a tutela da privacidade e a proteção das relações de consumo, assumindo obrigações e deveres quando explorarem atividades econômicas em mercados ricos em dados" (FALEIROS; MEDON, 2021, p. 961).

Observa-se que as decisões tomadas de forma híbrida, ou seja, envolvendo tanto automação quanto intervenção humana simultaneamente, não são contempladas pela previsão normativa. No entanto, é imperativo garantir o direito nessas situações complexas de decisão. Este estudo reconhece que, durante o processo decisório, há momentos em que ocorre a intervenção de uma pessoa natural ou a conclusão de decisões puramente humanas. É essencial assegurar o direito mesmo nessas circunstâncias, conforme argumentado pelas autoras Maria de Fátima Freire de Sá e Taisa Maria Macena de Lima:

> A regra do art. 20 da LGPD revela-se tímida na medida em que restringe o direito à explicação às decisões inteiramente automatizadas. Assim, as decisões que forem o resultado simultâneo da automação e da decisão humana não são alcançadas pela previsão normativa. Não há como ignorar, nos dias atuais, os processos decisórios complexos nos quais algumas fases são automatizadas e outras são implementadas com decisões puramente humanas. Tais processos decisórios são merecedores de igual cobertura legal (SÁ; LIMA, 2020, p.235).

O ordenamento jurídico brasileiro não estabelece um rol taxativo das hipóteses em que o processamento integralmente automatizado pode ocorrer, limitando-se a regulamentar o direito à explicação nos casos em que as decisões são tomadas sem interferência humana. A interpretação destes dispositivos deve ser realizada de forma sistêmica, considerando outros elementos normativos da própria LGPD, como os artigos 5º, 7º e 11, bem como dispositivos constitucionais e civilistas (BRASIL, 2018).

É fundamental ressaltar que a aplicabilidade do artigo 20 da LGPD não abrange todas as decisões automatizadas. As situações elencadas no caput do artigo devem ser interpretadas de forma exemplificativa, não exaustiva. Esta abordagem atribui significativa responsabilidade à ANPD, à doutrina jurídica e ao Poder Judiciário na tarefa de identificar e exemplificar situações em que o direito à explicação e à revisão podem ser invocados (MONTEIRO, 2018).

A ausência de um limiar específico de impacto na LGPD para caracterizar a relevância de uma decisão automatizada para o titular dos dados resulta em uma ampla abrangência normativa. Considera-se suficiente que a decisão afete os interesses do titular ou vise criar perfis relacionados a aspectos pessoais, profissionais, de consumo, de crédito ou de personalidade.

No âmbito dos algoritmos decisórios que processam dados pessoais, torna-se imperativo avaliar se o controlador está efetivamente respeitando e promovendo este direito fundamental, considerando as especificidades do objeto da decisão. Esta análise visa identificar possíveis práticas discriminatórias no tratamento automatizado de dados e verificar a adequada promoção do direito à proteção de dados, especialmente quando envolvem bens jurídicos que desempenham funções sociais constitucionalmente garantidas, como no caso exemplar da concessão de financiamento estudantil (MULHOLLAND; FRAJHOF, 2019).

Esta abordagem ampla da LGPD quanto às decisões automatizadas e perfis pessoais reflete uma tentativa de abranger as diversas formas em que o processamento automatizado de dados pode impactar os indivíduos. No entanto, também cria desafios interpretativos e de implementação, exigindo uma análise cuidadosa caso a caso para determinar quando e como as proteções da lei devem ser aplicadas.

Dentro de sua autonomia privada deve se encontrar o poder de escolher não estar sujeito a uma decisão tomada exclusivamente com base em tratamento automatizado que produza efeitos em sua esfera jurídica ou o afete significativamente. Maria de Fátima de Sá e Taisa Macedo de Lima argumentam que "pode-se extrair dessa norma o direito à explicação que se manifesta tanto como um direito individual do titular quanto como meio de supervisão" (SÁ; LIMA, 2020, p.234).

As mesmas autoras observam que, na ausência de qualquer vedação ao tratamento de dados totalmente automatizado, "a LGPD atribui direitos ao titular, contrapostos aos deveres do controlador" (SÁ; LIMA, 2020, p. 235).

A norma é de natureza permissiva[89], possibilitando o tratamento de dados sensíveis, incluindo dados de saúde e genéticos. Isso significa que, por exemplo, médicos e clínicas de saúde poderão, em teoria, realizar diagnósticos baseados exclusivamente em decisões algorítmicas.

Esta permissividade da norma, contudo, não isenta os controladores de dados de suas responsabilidades quanto à transparência do processo decisório. Estas explicações são fundamentais não apenas para avaliar a legitimidade e legalidade das decisões automatizadas,

[89] A norma permissiva expressa uma liberdade de ação, logo, a conduta do agente, nesse caso, não cria um risco proibido (GOMES, 2007).

mas também para estabelecer eventuais responsabilizações. Por exemplo, em avaliações de crédito baseadas em algoritmos, uma explicação adequada deve incluir informações sobre o perfil atribuído ao indivíduo, os dados utilizados no modelo estatístico e os potenciais consequências associadas a cada classificação.

Um exemplo concreto desta necessidade de reformulação pode ser observado no contexto do *credit scoring*. A relação entre o *credit scoring* e os conceitos trazidos pela LGPD merece especial atenção, particularmente quanto à perfilização e ao direito à explicação. Se inicialmente o STJ já havia estabelecido a necessidade de disponibilizar informações claras sobre critérios e variáveis do cálculo da pontuação creditícia, a LGPD expandiu significativamente estas exigências.

O direito à explicação, previsto no art. 20 da LGPD, vai além da mera transparência exigida pelo STJ, impondo às entidades a obrigação de fornecer informações sobre a lógica por trás das decisões automatizadas. Além de manter os requisitos de clareza e acessibilidade estabelecidos pelo Tribunal, a nova legislação acrescenta a necessidade de explicar como as variáveis influenciam o processo decisório e garante a possibilidade de revisão das decisões por pessoa natural (BRASIL, 2018).

Esta evolução normativa significa que as empresas agora devem não apenas informar as variáveis consideradas, como determinado pelo STJ, mas também explicar como estas impactam efetivamente a pontuação de crédito do consumidor, ressalvados os segredos comerciais e industriais. Trata-se de uma ampliação significativa do conceito original de transparência, visando garantir aos titulares dos dados uma compreensão mais profunda sobre como suas informações pessoais são utilizadas.

Para o enquadramento legal se faz fundamental que os agentes justifiquem o tratamento “a partir de pelo menos uma das bases legais, assim como criar toda uma estrutura que possa ser compatível com os deveres e princípios aos quais têm que se submeter” (FRAZÃO, 2021, p. 35).

A doutrina reconhece os avanços alcançados com a legislação protetiva de dados pessoais, embora observe que talvez não seja suficiente para criar um arcabouço completo. apesar de representar um progresso legislativo, os parâmetros legais para o exercício do direito à explicação podem não ser suficientes para assegurar a autonomia informativa do titular dos dados pessoais e para concretizar os princípios sistematizados no art. 6º, especialmente os princípios do livre acesso (inc. IV), da transparência (inc. VI) e da não discriminação (inc. IX) (LIMA, SÁ, 2020).

Esta complexidade tecnológica desafia os paradigmas tradicionais do direito, especialmente no campo da responsabilidade civil. O modelo clássico, fundamentado na tríade dano, nexo causal e culpa, mostra-se insuficiente diante das peculiaridades do tratamento automatizado de dados pessoais. A LGPD, reconhecendo esta nova realidade, demanda uma reformulação dos conceitos tradicionais de responsabilização para adequá-los a um contexto de riscos sistêmicos e danos potencialmente difusos.

5.4.4 Responsabilidade civil: entre a prevenção e a explicabilidade

A responsabilidade civil, como instituto jurídico voltado à compreensão e remediação dos males sociais, não pode se esquivar de abordar a questão da explicabilidade da IA. Em uma sociedade profundamente marcada pela evolução tecnológica, este instituto assume um papel fundamental, qual seja, servir como ponte entre o direito e a ética, estabelecendo parâmetros claros de responsabilização que considerem tanto a complexidade técnica quanto as implicações sociais das decisões automatizadas: “na sociedade tecnocientífica contemporânea, a responsabilidade representa o conceito base e integrador da ética e do direito. Isso porque tanto na ética, como no direito, é precisamente a responsabilidade que objetiva e formaliza os conceitos de liberdade e regulação” (NETTO; ROSENVALD, 2024, p. 7).

Este cenário é fruto da denominada "sociedade de risco", conceito cunhado por Ulrich Beck em 1980, para explicar o período pós-industrial ou pós-moderno em que "o sucesso da produção de riqueza foi ultrapassado pela produção do risco". Neste momento histórico, a atenção se volta para a análise do risco, onde "tudo se processa 'reflexivamente' em uma civilização que ameaça a si própria" (BECK, 1980; NETO, ROSENVALD, 2024, p.2).

Para compreender melhor essa mudança de paradigma social, Beck aprofunda sua análise ao estabelecer um contraste fundamental entre as sociedades moderna e contemporânea. Em sua perspectiva:

> Na obra desse sociólogo, abre-se o diálogo com o direito pelo viés da *segurança*. Esse é o vocábulo que exprime o reverso projeto normativo que serve de impulso para a sociedade de risco. Nas sociedades de classe que marcaram a modernidade havia o ideal da *igualdade* – consubstanciado por metas positivas de alteração social e acesso irrestrito À cidadania-, o qual foi substituído pelo sistema axiológico da sociedade *“insegura”*, uma utopia negativa e defensiva, pois já não mais se trata de alcançar efetivamente algo “bom”, mas tão somente de evitar o pior. O sonho da sociedade de classes é: todos querem e devem compartilhar do bolo. A meta da sociedade de risco é: todos devem ser poupados do veneno (BECK, 1980, p.42).

Beck argumenta que o ideal de igualdade das sociedades de classe modernas foi substituído pelo sistema axiológico da sociedade "insegura", uma utopia negativa e defensiva. O objetivo não é mais alcançar algo "bom", mas evitar o pior (BECK, 1980).

Contudo, apesar da visão pessimista de Beck, a sociedade evoluiu, reduzindo a subnutrição e aumentando a expectativa de vida[90]. Para Bauman observa:

> Vivemos indubitavelmente em algumas das sociedades mais seguras que já existiram, e, no entanto, ao contrário de evidências objetivas, nós – as pessoas mais mimadas e paparicadas de todas – nos sentimos ameaçados, inseguros e atemorizados, mais inclinados ao pânico e mais apaixonados por tudo que se refira à segurança e a proteção do que as pessoas da maioria das sociedades que se tem registro (BAUMAN, 2008, p.132).

Os indicadores de desenvolvimento humano apontam para avanços significativos em diversos aspectos da vida social, particularmente nas áreas de saúde pública, expectativa de vida e nutrição. Paradoxalmente, observa-se um incremento na percepção de insegurança e medo na sociedade contemporânea.

Gilles Lipovetsky identifica este fenômeno como uma manifestação do indivíduo contemporâneo "desestabilizado amplificando todos os riscos, obcecado por seus problemas pessoais, exasperado por um sistema repressivo julgado inativo ou 'clemente' demais, habituado a ser protegido e traumatizado por uma violência da qual ignora tudo: a insegurança". Esta análise revela uma complexa relação entre proteção social e percepção de vulnerabilidade (LIPOVETSKY, 2005, p.174).

Antes de adentrar no estudo da responsabilidade civil, é pertinente examinar, de forma sucinta, o conceito de risco adotado nesta pesquisa. De acordo com Gellert, risco pode ser definido como:

> Em poucas palavras, pode-se argumentar que o risco pode ter dois significados – um vernacular e outro mais técnico. No sentido vernacular, o risco é geralmente referido como um futuro, possível perigo, ou seja, como "um perigo eventual que pode ser previsto apenas até certo ponto" (GODARD *et al*., 2002, p. 12). No sentido técnico, no entanto, o risco pode ser visto como uma noção dupla. Isto é usado para tomada de decisão com base na avaliação de futuros eventos. Seus elementos constitutivos são duas operações distintas e unidas: prever eventos futuros (negativo e positivos) e tomar decisões com base nisso. Portanto, pode-se argumentar que 'qualquer decisão relacionada ao risco envolve dois e, ainda assim, elementos inseparáveis: os fatos

[90] A expectativa de vida ao nascer no Brasil passou de 36,5 anos em 1930 para 69,9 anos em 2000. No período entre 2000 e 2010, essa expectativa subiu mais 4 anos, alcançando 73,9 anos. Especificamente entre as mulheres, o aumento foi de 3,7 anos, enquanto entre os homens foi de 4,2 anos. Em 2010, a média de vida das mulheres era de 77,6 anos, e a dos homens, 73,9 anos. Enquanto em 2022, a expectativa de vida subiu para 75,5 anos (IBGE, 2023).

> objetivos e uma visão subjetiva sobre a conveniência do que deve se ganhar, ou perder, pela decisão' (GELLERT, 2017, p.2).

Na perspectiva de Raffaele De Giorgi, o conceito de risco estabelece uma relação singular entre futuro e sociedade, fundamentando a construção de estruturas nos processos de transformação sistêmica. O autor caracteriza o risco como uma construção essencialmente comunicativa, que reflete a possibilidade de arrependimento futuro relacionado a escolhas que resultaram em danos que se pretendia evitar (GIORGI, 2005).

A noção de "sociedade de risco" emerge como um paradigma que transcende a mera reformulação do entendimento sobre progresso e modernidade, evidenciando as complexidades inerentes à gestão de riscos contemporâneos. Neste contexto, o risco demanda um cálculo temporal em condições onde os instrumentos tradicionais de racionalidade e estatística se mostram insuficientes.

A relação entre risco e contingência revela-se indissociável da conexão entre risco e complexidade, estabelecendo princípios geradores de formas, distinções e vínculos que constituem a realidade observável. Raffaele De Giorgi enfatiza que a alternativa ao risco não reside na segurança, argumentando que a busca por segurança representa uma negação da contingência através da construção de estabilidades artificiais (GIORGI, 2005).

A experiência demonstra que o incremento em medidas de segurança frequentemente resulta na emergência de novos tipos de risco, configurando um cenário de imprevisibilidade. Esta dinâmica pode ser observada nas consequências das políticas de segurança implementadas globalmente e nas implicações das medidas introduzidas pelo direito penal dos Estados nacionais (GIORGI, 2005).

No contexto da evolução tecnológica, particularmente no desenvolvimento dos sistemas robóticos inteligentes, estas dinâmicas assumem nova complexidade. A IA, com suas capacidades de aprendizado e adaptação, introduz questões fundamentais sobre responsabilidade, ética e governança. A regulação destes sistemas requer uma abordagem holística que considere não apenas os riscos tecnológicos inerentes, mas também seus impactos sociais, econômicos e éticos.

O risco, no contexto da proteção de dados, possui um caráter predominantemente subjetivo, uma vez que a partir dos riscos identificados no programa de compliance[91], o "controlador deverá tomar uma decisão sobre quais riscos deseja assumir em seu negócio, mesmo estando sujeito a eventual sanção prevista em lei" (GOMES, 2019, p. 10).

[91] Este trabalho aprofundará o estudo do *compliance* mais a frente.

Compreendido o conceito de risco e suas implicações no contexto social, é possível analisar como a responsabilidade civil se adapta e evolui para responder a estes novos desafios. Neste novo formato social, a responsabilidade civil assume outros contornos, garantindo a "tutela da intangibilidade existencial e patrimonial" que "não autoriza sermos expostos por a danos, riscos ou ameaças que excedam aquilo que se justifique em sociedade". Transformando em um representante de uma forma preventiva do risco, antecipando resultados e colocando no centro do ordenamento todos aqueles que potencialmente podem ser vítimas[92](NETTO; ROSENVALD, 2024, p. 8).

Há a necessidade para que esta perspectiva transcende a mera compensação de danos, orientando-se para a promoção de “comportamentos meritórios, especialmente os deveres positivos de evitar e mitigar danos – reduzindo as consequências” (NETTO; ROSENVALD, 2024, p. 9).

Para Nelson Rosenvald e Felipe Braga Netto o ordenamento jurídico brasileiro apresenta importantes avanços nessa direção, evidenciados em diversos aspectos. A imputação objetiva de danos, fundamentada no parágrafo único do art. 927[93] do CC estabelece uma conexão direta com o princípio constitucional da solidariedade, determinando a obrigatoriedade de reparação como imperativo de segurança social, especialmente em atividades que apresentam riscos inerentes (NETTO; ROSENVALD, 2024).

Consequentemente, o nexo de causalidade experimenta uma expansão conceitual, ultrapassando a tradicional causalidade natural para abarcar uma dimensão jurídica mais abrangente. Esta nova perspectiva permite o reconhecimento da responsabilidade em situações de risco hipotético ou de danos provocados por grupos indeterminados de agentes, sem a necessidade de identificação específica do causador direto da lesão (NETTO; ROSENVALD, 2024).

O sistema de proteção civil contemporâneo reconhece novas categorias de danos merecedores de tutela jurídica, superando a tradicional dicotomia entre danos patrimoniais e morais. Surgem, assim, modalidades mais específicas como o dano estético, o dano existencial e a perda de uma chance, cada qual com características e requisitos próprios de configuração.

Em um momento social, onde as relações sociais são progressivamente mediadas por tecnologias que transformam comportamentos em dados, torna-se imperativo repensar os paradigmas tradicionais da responsabilidade civil. Esta necessidade de adaptação reflete a própria natureza dinâmica do instituto, que deve responder adequadamente aos desafios

[92] Contrário ao antropocentrismo que coloca a vítima no centro do ordenamento.
[93] Art. 927. Aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo (BRASIL, 2002).

impostos pela sociedade contemporânea, transcendendo os limites estabelecidos no art. 944 do CC[94].

Portanto, o conceito de responsabilidade civil deve se adequar aos novos formatos sociais, visto que é "por essência cambiante, extremamente sensível aos influxos econômicos e sociais". No contexto do capitalismo de vigilância, onde "a própria sociedade se torna objeto de extração e controle e nossa vida é reduzida a dados comportamentais", é necessário reconduzir a responsabilidade para novos olhares que vão além do previsto no texto civil (NETTO; ROSENVALD, 2024, p. 16, 18).

A complexidade das relações jurídicas atuais demanda uma responsabilidade civil mais sofisticada e adaptável, capaz de oferecer respostas efetivas aos novos conflitos e garantir a proteção integral dos direitos fundamentais. Este processo de evolução contínua reflete a necessidade de harmonização entre os princípios tradicionais da responsabilidade civil e as emergentes demandas sociais do século XXI.

Neste ponto, destaca-se que a ideia de responsabilidade civil se encontra com os conceitos de *privacy by design* e *privacy by default*. Aquela é conceituada como a necessidade do agente ao "realizar qualquer tipo de tratamento de dados pessoais, deve pensar na privacidade em cada passo, o que inclui projeto, desenvolvimento de produtos e softwares, sistemas de informática", com a finalidade garantir a privacidade durante todo o ciclo de tratamento. Enquanto, esta representa que "ao lançar qualquer produto ou serviço ao público, as regras mais protéticas de tutela da privacidade devem ser aplicadas, sem que se exija do usuário qualquer iniciativa para tal propósito" (FRAZÃO, 2024, p. 48).

Há, por outro lado, o desafio de lidar com o poder e com a influência exercidos pelas das grandes corporações que operam em mercados ricos em dados (*data-rich markets*). Estas empresas, detentoras do controle sobre a arquitetura e programação das plataformas digitais, frequentemente utilizam algoritmos complexos e opacos, muitas vezes referidos como 'caixas-pretas', para processar e analisar dados pessoais em larga escala (DE LUCCA, 2014).

Este contexto evidencia uma notável assimetria de poder entre estas corporações e as instituições estatais, frequentemente caracterizada pela fragilidade dos mecanismos regulatórios e fiscalizatórios. A sociedade está inserida em um contexto em que as estruturas oligopolistas[95] exercem significativa influência sobre os mecanismos de precificação, enquanto

[94] Art. 944. A indenização mede-se pela extensão do dano. Parágrafo único. Se houver excessiva desproporção entre a gravidade da culpa e o dano, poderá o juiz reduzir, equitativamente, a indenização (BRASIL, 2002).

[95] Oligopólio é a situação em que um número restrito de empresas detém o controle da maior parte do mercado (MICHAELIS, 2024).

as estratégias de publicidade e marketing atingem níveis de persuasão sem precedentes, demandando o estabelecimento de marcos regulatórios para a proteção efetiva dos titulares de dados pessoais (FALEIROS; MEDON, 2021).

A problemática do combate às práticas discriminatórias no ambiente digital emerge como elemento central nesta discussão, "considerando seu potencial impacto sobre direitos humanos fundamentais". A implementação indiscriminada de algoritmos e técnicas de perfilamento pode resultar em processos decisórios que apenas mantém, mas amplificam as desigualdades existentes, afetando de maneira desproporcional grupos em situação de vulnerabilidade (FALEIROS; MEDON *apud* ZARREHPARVAR, 2006, p. 233).

O enfrentamento destes desafios requer a implementação de estruturas de governança adequadas às especificidades das relações jurídicas de consumo no contexto digital, com ênfase particular nas contratações eletrônicas. Estas estruturas devem ser concebidas para assegurar princípios fundamentais como transparência, responsabilização e conduta ética no processamento de dados pessoais e nas práticas comerciais digitais.

Uma abordagem fundamental neste contexto é a adoção do princípio da minimização de dados (*data minimization*), alinhado com o conceito de "*privacy by default*". Esta abordagem pressupõe que as entidades responsáveis pela coleta e tratamento de dados pessoais devem limitar estas operações ao mínimo necessário, estabelecendo configurações predefinidas que priorizem a privacidade dos usuários, promovendo assim uma cultura de proteção à privacidade desde a concepção dos sistemas e serviços digitais (FALEIROS, MEDON, 2021).

A efetividade das medidas regulatórias depende significativamente da capacidade de *enforcement*[96] por parte das autoridades reguladoras e concorrenciais. O acesso aos mecanismos internos das empresas, incluindo seus algoritmos e práticas de tratamento de dados, pode ser crucial para garantir a conformidade com as normas de proteção de dados e direitos do consumidor. Este tipo de "fiscalização ativa é essencial para equilibrar o poder entre as grandes corporações de tecnologia e os interesses públicos representados pelo Estado" (FALEIROS; MEDON, 2021, p. 966).

Por todo este exposto, a LGPD consagrou o dever de segurança de dados, previsto no art. 46[97], impondo aos agentes de tratamento o dever de zelar pelos seus sistemas.

---

[96] Em tradução livre, cumprimento do regramento.

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

§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do

> Padrões éticos e de moralidade precisam ser estabelecidos para que um mínimo de segurança exista no desenvolvimento das relações interativas na realidade virtual digital. Tal indicação é necessária, pois desenvolver-se por meio da interação com elementos exógenos e endógenos não é uma opção para o ser humano, mas, sim, um caminho inescapável. Contudo, nesse contexto, algumas perguntas que se sobressaem são: até quando, de que forma e qual será o preço desse desenvolvimento do ser humano ante as realidades virtuais que cria? (FALEIROS; MEDON, 2021, p. 962)

A partir desta compreensão do dever de segurança de dados, é possível avançar para uma análise mais detalhada das três dimensões fundamentais da responsabilidade no contexto digital. O primeiro conceito é o "*liability"*, a visão clássica que diz respeito à eficácia condenatória de uma sentença, decorrente da análise do nexo causal entre uma conduta e um dano. Esse entendimento é enriquecido por outros elementos, levando em consideração o nexo causal de imputação concreto e as particularidades de cada jurisdição. Trata-se de uma manifestação *ex post*[98], apresentando-se após a ocorrência do dano (NETTO; ROSENVALD; 2024).

A responsabilidade é solidária entre controlador e operador, "que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais" (BRASIL, 2018).

A responsabilidade civil do controlador é objetiva, conforme previsto no art. 43, não dependendo da discussão, tão pouco de comprovação de culpa, "irrelevante, pois, que o controlador tenha atuação diligente no tratamento de dados ou extremo zelo na escolha dos colaboradores aos quais delegue essa tarefa" (SÁ; LIMA, 2020, p. 237).

No mesmo artigo, a Lei prevê 3 (três) circunstâncias nas quais o dever de indenizar será excluído, se comprovarem que, não realizaram o tratamento de dados pessoais que lhes é atribuído (I); que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados (II); ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros (III).

Ressalta-se que, "a existência de motivo legítimo para não fornecer a explicação sobre a decisão automatizada não afasta o direito do titular de dados de ser indenizado, caso fique

---

tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

§ 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018).

[98] *Ex post* é um termo em latim que significa "após o fato".

evidenciado que houve dano" (SÁ; LIMA, 2020, p. 237). Ou seja, a necessidade de proteger o segredo comercial ou industrial não excluiu a reparação civil.

No que diz respeito aos agentes públicos, a LGPD não aborda explicitamente a questão da culpa ou do risco. No entanto, é fundamental analisar a legislação em conjunto com outras normas do ordenamento jurídico brasileiro. A CF, por exemplo, estabelece no art. 37, parágrafo 6º[99], que a culpa não é requisito para atribuir ao agente público o dever de reparar os danos decorrentes da violação de dados pessoais. Essa disposição constitucional reforça a responsabilidade objetiva dos agentes públicos em relação à proteção dos dados, independentemente de culpa ou dolo:

> Afinal, a norma constitucional prevê a responsabilidade, na modalidade objetiva, para os entes de direito público, pertencentes ao quadro administrativo. Por conseguinte, tanto os agentes privados como os agentes públicos respondem objetivamente pela violação de direitos, no tratamento de dados pessoais. (SÁ, LIMA, p. 237).

A LGPD possui sessão específica para o tema da responsabilidade civil, prevista no Capítulo VI, a qual merece atenção e um tópico específico para estudo, pois elenca novos conceitos e formas de responsabilização civil, adotando a "concepção funcionalizada da responsabilidade civil", sem esquecer da função compensatória, com ênfase na função precaucional (SÁ; LIMA, 2020, p. 236).

Ao analisar o art. 46 previu:

> [...] para a tutela da responsabilidade civil em razão de danos decorrentes desse valor imperativo (segurança dos dados), delimitando um critério geral de imputação lastreado na verificação, no mapeamento e na demonstração dos resultados e riscos do tratamento, sob pena de se ter um tratamento irregular de dados (art. 44, II, LGPD) na prestação de serviços por parte dos provedores, com emanação lastreada na ruptura de uma expectativa legítima (que ultrapassa a concepção de 'defeito') quanto à segurança dos processos de coleta, tratamento e armazenagem de dados (FALEIROS; MEDON, 2021, p. 962).

Essa norma é similar ao GDPR que coaduna com os fundamentos como sendo o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o direito ao livre desenvolvimento da personalidade, o desenvolvimento econômico e tecnológico, a livre iniciativa, a livre concorrência e a defesa do consumidor (CORDEIRO, 2020).

---

[99] § 6º. As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa (BRASIL, 1988).

Diante desta profundidade do conceito que autores como Felipe Braga Netto e Nelson Rosenvald recorrem a conceitos do *common law*[100] , propondo uma "polissemia da responsabilidade civil". É importante notar que a visão compensatória clássica do ordenamento jurídico brasileiro não é abandonada, mas complementada por novas perspectivas (NETTO; ROSENVALD, 2024).

A responsabilidade civil agora se posiciona não apenas como um mecanismo de contenção de danos, mas também como uma fórmula para contenção de comportamentos (NETTO; ROSENVALD, 2024).

A LGPD é um exemplo legislativo neste sentido:

> Em sintonia com o pensamento de Bart van der Sloot, que reconhece a 'privacidade como virtude', agregam-se a pessoa do agente e a indução à conformidade mediante uma regulação de gestão de riscos, em especial com vistas à sua mitigação por parte de um desenvolvedor de tecnologias digitais emergentes que atua como um agente de tratamento de dados pessoais e que deve observar verdadeira plêiade de deveres preventivos dos quais emanam variadas funções da responsabilidade civil (em especial, *accountability* e *answerability*). (NETTO; ROSENVALD, 2024, p. 33)

Os autores Nelson Rosenvald e Felipe Braga Netto introduzem três conceitos adicionais: '*responsibility'*, '*accountability*' e '*answerability'*. Embora todos possam ser traduzidos como "responsabilidade" em português, na prática "transcendem a função judicial de desfazimento de prejuízos, conferindo novas camadas à responsabilidade, capaz de responder à complexidade e velocidade dos arranjos sociais". Este estudo perpassará por todos, mas o foco será a *answerability* (NETTO; ROSENVALD, 2024).

Dentre estas três dimensões, a *responsibility* merece atenção por seu caráter preventivo e sua relação direta com a proteção de direitos fundamentais, extrapolando os cuidados das autoridades, referindo-se à "decisão diária posta a cada pessoa em seu dever de não interferir indevidamente na esfera alheia", tendo um caráter *ex ante*[101](NETTO; ROSENVALD; 2024, p. 23).

No contexto do capitalismo de vigilância, a *responsibility* apresenta duas vertentes. A primeira refere-se à obrigação de fornecer educação digital aos titulares de dados, conforme previsto no art. 26 da Lei 12.925/14[102]. A falta de conhecimento sobre o destino dos dados torna o usuário incapaz de protegê-los.

---

[100] *Common law* (do inglês "direito comum") é o direito que se desenvolveu em certos países por meio das decisões dos tribunais, e não mediante atos legislativos ou executivos.

[101] *Ex ante* é uma expressão latina que significa "antes do fato".

[102] Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e

Como observa Renato Opice Blum, a aprovação de leis para garantir maior segurança aos usuários da internet será ineficaz sem educação digital prévia. Esta educação deve começar na fase escolar e continuar por toda a vida, dada a natureza dinâmica do mundo virtual:

> [...] pouco adiantará a aprovação de leis para garantir a aprovação de leis para garantir uma segurança maior ao usuário da rede mundial de computadores se ele, antes de iniciar a conexão com um mundo tão rico, tão vasto, tão cheio de informações, mas por vezes perigoso, não for educado digitalmente. Primeiro, é necessário que o usuário, tanto no âmbito pessoal, quanto profissional, e de forma preventiva, seja educado para isso. Por meio de educação voltada para o uso correto da Internet e suas informações. Esse aprendizado deverá começar na fase escolar e perdurar por toda a vida do ser humano, ante o dinamismo e a abrangência do mundo virtual. Da mesma forma, as escolas devem fazer uso de uma Política de Segurança da Informação, aplicando sistemas eficientes opara resguardar o sigilo de suas informações, especialmente de seus alunos. Entretanto, é impossível observar que de nada adiantará a escola empresa ter uma estrutura adequada na área de Tecnologia da Informação se os professores, alunos e pais não tiverem consciência da importância de se garantir a segurança da informação (BLUM, 2015, p.189-190).

O princípio da autodeterminação informativa, previsto no art. 2º, II, da LGPD[103], é fundamental neste contexto. Segundo Fabiano Menke, este princípio, juntamente com o respeito à privacidade, tem a relação mais próxima com a disciplina da proteção de dados pessoais, sendo o único no rol dos incisos do dispositivo que tem sua origem atrelada a esta matéria (MENKE, 2020).

No âmbito da tecnologia, especialmente no que tange à proteção de dados, é notória a prevalência de termos em inglês, mesmo quando existem equivalentes em português. Expressões como *input* e *privacy by design*[104]*,* são frequentemente utilizadas, refletindo uma tendência global na área. Este fenômeno linguístico pode ser analisado à luz da observação de Harari sugere que "as pessoas comuns não talvez não compreendam a IA, mas percebem que o futuro as está deixando para trás" (HARARI *apud* NETTO; ROSENVALD; 2024, p. 25).

Esta percepção de distanciamento entre o indivíduo comum e as inovações tecnológicas ressalta a importância da autodeterminação informativa. Felipe Braga Netto e Nelson Rosenvald enfatizam que o objetivo primordial é "a atribuição, ao titular, da inexorável liberdade para que direcione os sentidos do tratamento atribuído a seu acervo de dados que flui pelas redes" (NETTO; ROSENVALD, 2024, p.25).

---

responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico (BRASIL, 2014).

[103] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: [...] II - a autodeterminação informativa (BRASIL, 2018);

[104] *Privacy by design*, em tradução livre, significa a privacidade desde a concepção. O conceito será apresentado e aprofundado capítulo de responsabilidade civil.

Tal conceito coloca o indivíduo no centro do controle sobre suas próprias informações digitais:

> É possível dizer, que dos fundamentos presente no art. 2º da LGPD, a autodeterminação informativa é aquela que guarda, juntamente com o respeito à privacidade, a relação mais próxima com a disciplina da proteção de dados pessoais. Isso porque consiste no único presente no rol dos incisos do dispositivo que tem a sua origem atrelada a esta matéria, que nos dias de hoje ganhou contornos de autonomia. (MENKE, 2020)

No âmbito da proteção de dados e da ética digital, o conceito de *responsabilty* assume uma dimensão mais ampla, que "se dirige aos agentes de tratamento, significando a inserção da ética no exercício da sua atividade". Esta perspectiva enfatiza a importância de uma conduta ética por parte dos responsáveis pelo tratamento de dados pessoais (NETTO; ROSENVALD, 2024, p. 25).

Um aspecto crucial desta responsabilidade é a noção de *accountability*, que pode ser compreendida como uma vertente que engloba "parâmetros regulatórios preventivos, que promovem uma interação entre a *liability* do CC com uma regulação voltada à governança dos dados, seja em caráter *ex ante* ou *ex post*. Este conceito pode ser interpretado de diversas formas, incluindo responsabilização, prestação de contas, fiscalização, sanção ou *answerability* (NETTO; ROSENVALD, 2024;AUGUSTO; RIZZARDI, 2014).

Assim, a terminologia renova-se para adotar contornos preventivos, uma congruência entre os modelos europeu e brasileiro:

> O modelo jurídico da responsabilidade civil é por essência cambiante, extremamente sensível aos influxos econômicos e sociais. Na sociedade de riscos, um altivo papel do ordenamento jurídico consiste em induzir, de forma generalizada, comportamentos virtuosos, orientando potenciais ofensores a adotar medidas de segurança a evitar condutas danosas. Uma ode à virtude da 'previdência' (olhar antes). (ROSENVALD; OLIVEIRA, 2019, p. 331)

Consequentemente, a responsabilização por tratamento irregular de dados[105] que contempla múltiplas dimensões das "ações cabíveis e regularmente esperadas do respectivo agente para que seja possível promover o reequilíbrio das tensões causadas durante tais operações e que culminem na perda da autodeterminação informativa", em outras palavras, "em

[105] Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano (BRASIL, 2018).

verdadeira manipulação do controle exercido pelo consumidor sobre sua decisão" (FALEIROS; MEDON, 2021, p. 965).

Nesta direção, os autores José Faleiros e Filipe Medon realizam uma ligação entre o CDC e a LGPD, no sentido de que, a norma mais recente protetiva dos dados, não afasta as normas consumeristas, principalmente o previsto no art. 45[106], "em verdade, revela a necessidade de verdadeiro diálogo de fontes a fim de efetivar a proteção do ciber-consumidor" (FALEIROS; MEDON, 2021, p. 965).

A relação entre *accountability* e transparência é objeto de debate acadêmico. Enquanto alguns estudiosos as consideram sinônimos ou relacionadas, outros preferem diferenciá-las. No contexto das decisões algorítmicas, por exemplo, a transparência, embora necessária, não é suficiente por si só, sendo fundamental exigir uma explicação mais aprofundada. A transparência refere-se à divulgação de certas informações sobre um sistema de IA, enquanto a explicação aborda os fatores que influenciam o resultado do sistema (ZARSKY, 2013; DOSHI-VELEZ; KAMINSKI, 2019b; KORTZ, 2017).

É importante notar que a mera disponibilização do código-fonte nem sempre é eficaz para atender aos requisitos de transparência e explicabilidade. A prestação de contas assume um papel fundamental na regulação e estabelecimento de sistemas de IA legítimos, justos e funcionais. Neste contexto, o direito à explicação tem se destacado como um mecanismo para implementar a prestação de contas, ganhando relevância em áreas como moderação de conteúdo em redes sociais e pontuação de crédito (ANANNY; CRAWFORD, 2018; KAMINSKI, 2019b; DOSHI-VELEZ; KORTZ, 2017).

No que diz respeito à aplicação *ex ante* esta se manifesta através de orientações para controladores[107] e operadores[108] de dados, "mediante a inserção de regras de boas práticas que estabeleçam os procedimentos, normas de segurança e padrões técnicos, tal como se extrai do

[106] Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente (BRASIL, 2018).

[107] Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (BRASIL, 2018).

[108] Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (BRASIL, 2018).

artigo 50 da LGPD[109]". Isso implica na adoção de regras de *compliance*[110], um conceito que remete à conformidade com os parâmetros regulatórios que equilibram a proteção da privacidade e o direito à concorrência (NETTO; ROSENVALD, 2024, p. 26).

A legislação brasileira de proteção de dados incorpora este princípio em diversos momentos, como no artigo 6º, X[111], que estabelece o princípio da "responsabilização e prestação de contas". De forma similar, o GDPR garante aos *stakeholders*[112] o direito de serem informados sobre operações de dados que possam impactar o livre desenvolvimento da personalidade, causar discriminação ou violar a dignidade e o exercício da cidadania[113].

Quanto à aplicação *ex post*, esta serve como um guia para magistrados e outras autoridades, auxiliando na identificação e quantificação de responsabilidades, bem como no estabelecimento de remédios mais adequados:

> Assim, ao invés do juiz se socorrer da discricionariedade para aferir o risco intrínseco de uma certa atividade por sua elevada danosidade (parágrafo único, art. 927 do CC) – o desincentivo ao empreendedorismo é a reação dos agentes econômicos à insegurança jurídica – estabelecem-se padrões e garantias instrumentais que atuam como parâmetros objetivos para a mensuração do risco em comparação com outras atividades. (NETTO; ROSENVALD, 2024, p. 27)

---

[109] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

[110] O termo *compliance* tem origem na língua inglesa, do termo *to comply*, que representa a expectativa de adesão e conformidade com os parâmetros regulatórios que elucidam entre a tutela da privacidade e o direito de concorrência.

[111] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:[...] X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

[112] Em tradução livre, o termo stakeholders significa partes interessadas. É um dos termos utilizados em diversas áreas como gestão de projetos, comunicação social administração e arquitetura de software referente às partes interessadas que devem estar de acordo com as práticas de governança corporativa executadas pela empresa.

[113] **Artigo 14º - Informação a ser fornecida quando os dados pessoais não forem obtidos junto ao titular dos dados. Nos casos em que os dados pessoais não forem obtidos junto ao titular dos dados, o responsável pelo tratamento deverá fornecer ao titular dos dados as seguintes informações:** A identidade e os contatos do responsável pelo tratamento e, se for o caso, do seu representante; Os contatos do encarregado da proteção de dados, se for caso disso; As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento; As categorias dos dados pessoais em questão; Os destinatários ou categorias de destinatários dos dados pessoais, se for o caso; Quando aplicável, que o responsável pelo tratamento tenciona transferir dados pessoais para um destinatário em um país terceiro ou uma organização internacional, e a existência ou a ausência de uma decisão de adequação pela Comissão, ou, no caso de transferências referidas no artigo 46.º ou 47.º, ou no segundo parágrafo do artigo 49.º, uma referência às garantias adequadas ou apropriadas e aos meios para obter uma cópia das mesmas ou onde foram disponibilizadas (EUROPA, 2018).

Em suma, a *accountability* no contexto da proteção de dados representa um princípio fundamental que promove o equilíbrio entre inovação tecnológica e respeito aos direitos individuais.

Após compreender o papel da *accountability*, é fundamental examinar o conceito de *answerability*, que representa uma evolução significativa na forma como entendemos a responsabilidade no contexto da IA. O conceito de *answerability* ou *explainability* (explicabilidade) emerge como um forte ponto na intersecção entre a proteção de dados e a ética da IA. Nelson Rosenvald e Felipe Braga Netto definem a explicabilidade como o "dever recíproco de construção da fidúcia a partir do imperativo da transparência". Esta noção transcende a mera obrigação de informar, constituindo-se como um direito dos indivíduos de "exigir razões para que ações e decisões sejam tomadas por aquele que exerce o controle da atividade" (NETTO; ROSENVALD, 2024, p. 28).

A LGPD incorpora este princípio em seu artigo 6º, VI, estabelecendo a transparência como um pilar fundamental. Esta abordagem relacional reconhece não apenas a responsabilidade do agente que trata os dados, mas também o direito do titular dos dados de compreender e questionar as decisões que o afetam (NETTO; ROSENVALD, 2024).

Verifica-se que, a explicação prevista no art. 20, implementa novos limites da responsabilidade, “não é apenas fazer algo e saber o que você está fazendo; é também uma questão comunicativa, talvez até dialógica, pois a sociedade, deseja respeitar os seres humanos não apenas como seres autônomos, mas também sociais”. A integração da IA no processo decisório deve sempre considerar a indispensável participação humana para garantir a transparência e a responsabilidade. (NETTO; ROSENVALD, 2024, p. 29)

Mark Coeckelbergh levanta questões pertinentes sobre a natureza das explicações necessárias, que direcionam para a complexidade da implementação prática da explicabilidade em sistemas de IA destacando a necessidade contínua de participação humana para garantir transparência e responsabilidade:

> Mas as pessoas precisam de explicações ou precisam de razões? Explicações podem contar como razões e, em caso afirmativo, quando? A responsabilidade como prestação de contas também pode ser formulada em termos de razões, ou mais especificamente, em termos de dar razões. E então, para razões, parece valer o mesmo que para explicações em geral: assumindo que apenas os humanos podem realmente dar razões, a IA responsável significa que os humanos devem assumir essa tarefa. O desenvolvimento da IA deve, então, apoiar essa tarefa humana de dar razões àqueles que fazem perguntas sobre as ações e decisões mediadas pela tecnologia. (COECKELERGH, 2020, p. 2051)

Pelo exposto, verifica-se que a *answerability* ultrapassa o conceito do direito de informação, “é um procedimento recíproco de justificação de escolhas”. O desafio reside em buscar uma resposta ontológica, fundamentada na identificação da pertinência das funções preventivas e precaucionais da responsabilidade civil, para que se possa aferir a expectativa depositada sobre cada participante da atividade, especialmente no que diz respeito à previsibilidade de eventuais consequências. Conclui-se que a clareza na definição dessas funções é essencial para estabelecer um sistema de responsabilidade civil que atenda às expectativas e minimize riscos (NETTO; ROSENVALD, 2024, p. 29).

Nesse sentido, a doutrina tem equiparado com a necessidade e a explicação da IA com a mesma requerida na tomada de decisão humana, como ocorre nas decisões judiciais:

> Com efeito, sempre nos pareceu razoável em ordenamentos democráticos que o agente fosse capaz de explicar a vítima porque ele praticou uma ação específica, tomou uma decisão ou recomendou algo. Por exemplo, pode-se pedir a um juiz que fundamente a sua decisão ou demandar de um criminoso a explicação de suas ações. Se a regra é que o interessado é uma pessoa capaz de pedir e entender explicações, é também legítimo que pessoas também exijam uma explicação em nome de um não humano ou mesmo em nome de outros humanos carentes de cognição. As decisões e ações humanas precisam se explicáveis se quiserem ser responsáveis – olhando para o passado e no presente (NETTO; ROSENVALD, 2024, p. 29).

O art. 20 da LGPD aprofunda esta noção ao garantir ao titular de dados pessoais o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado. Isto se estende a decisões que impactam o perfil pessoal, profissional, de consumo e de crédito do indivíduo. A partir da interpretação deste artigo, esta provisão efetivamente se converte em uma *ability to appeal*[114], fortalecendo significativamente os direitos dos titulares de dados (CORDEIRO, 2021, p. 26).

A explicabilidade, neste contexto, vai além de uma simples prestação de informações. Trata-se de um procedimento de justificação de escolhas, ou seja, confere ao titular o direito de "se opor ao seu *profiling*, apagá-lo, retificá-lo ou contestar as decisões automatizadas a ele relativas". Este conceito encontra paralelos em outras áreas do direito, como na fundamentação de decisões judiciais, onde se espera que os agentes sejam capazes de explicar suas ações e decisões (NETTO; ROSENVALD, 2024, p. 29).

---

[114] No contexto jurídico, ability to appeal refere-se à capacidade ou ao direito de uma parte envolvida em um processo judicial de recorrer de uma decisão tomada por um tribunal ou juiz a uma instância superior. Esse direito é um elemento fundamental do devido processo legal, garantindo que as partes possam contestar decisões que considerem injustas ou incorretas.

Na prática, a implementação destes princípios pode ser observada em empresas como a Uber, que permite que motoristas obtenham explicações e solicitem revisões de desativações automáticas realizadas por algoritmos. Este exemplo ilustra como a explicabilidade pode ser operacionalizada no contexto de decisões automatizadas que afetam diretamente os indivíduos.

O GDPR, no artigo 22[115], estabelece o *right to an explanation*[116], que impõe ao controlador o dever de implementar salvaguardas ao desenhar decisões automatizadas, implicando que a "decisão deva ser explicada de uma forma que o sujeito possa compreender o resultado, o que não requer necessariamente que 'black box' seja aberta", mas sim em fornecer uma explicação compreensível que oriente o titular sobre como um resultado diferente poderia ser alcançado (NETTO; ROSENVALD, 2024, p. 30).

A materialização destes conceitos teóricos pode ser melhor compreendida através da análise de casos concretos que demonstram como os tribunais e instituições têm lidado com estas questões. Um caso emblemático no Brasil foi a prática de *geo pricing* e *geo blocking,* definida como as "práticas que consideram a localização geográfica para precificação algorítmica, mas com nuances próprias", praticado pela empresa Decolar.com no Ocasião dos Jogos Olímpicos do Rio de Janeiro, em 2016[117]. O Ministério Público do Estado do Rio de

[115] Art. 22. 1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar. 2. O n.o 1 não se aplica se a decisão: a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento; b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou c) For baseada no consentimento explícito do titular dos dados. 3. Nos casos a que se referem o nº 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão. 4**.** As decisões a que se refere o n.o 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.o, n.o 1, a não ser que o n.o 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular (EUROPA, 2018).

[116] Em tradução livre, significa direito à explicação.

[117] O caso em questão representa um marco significativo na atuação do Ministério Público em defesa dos direitos dos consumidores no âmbito digital, especialmente no que tange às práticas comerciais de empresas de e-commerce. Este episódio, que envolveu a empresa "Decolar.com", ilustra a complexidade dos desafios enfrentados na regulação do comércio eletrônico e a importância da vigilância constante por parte dos órgãos de proteção ao consumidor. A investigação teve início com a atuação diligente do Promotor de Justiça Dr. Guilherme Magalhães Martins, então titular da 5ª Promotoria de Tutela Coletiva do Consumidor da Capital, vinculada ao Ministério Público do Estado do Rio de Janeiro. A iniciativa do Dr. Martins demonstra a proatividade do Ministério Público em identificar e investigar práticas potencialmente lesivas aos consumidores no ambiente digital. O processo investigativo culminou na instauração do inquérito civil nº 347/2016, um procedimento administrativo que visa coletar evidências e informações para fundamentar possíveis ações judiciais. Esta etapa é crucial para a construção de um caso sólido, permitindo aos promotores reunir provas substanciais sobre as práticas comerciais da empresa investigada. Subsequentemente, com base nas evidências coletadas durante o inquérito civil, foi proposta uma ação civil pública (nº 0111117-27.2019.8.19.0001) contra a "Decolar.com". É importante ressaltar que nesta fase, o caso contou também com a participação do Promotor de Justiça Dr. Pedro Rubim Borges Fortes, cuja expertise adicional contribuiu para fortalecer a argumentação

Janeiro denunciou a empresa por apresentar “precificação variável a depender da localização de acesso à plataforma do potencial consumidor”. Este caso abriu uma discussão mais amplamente os limites de tais aferições, de sua utilização e a necessidade de que se conceba uma resposta, pelos direitos fundamentais, à predição algorítmica de comportamentos (FALEIROS, MEDON, 2021, p. 955).

Esse caso demonstrou que é possível acessar e fornecer uma explicação sem a necessidade de acessar o código fonte, distanciando do debate que envolve a proteção ao segredo industrial.

> É possível reproduzir o comportamento do algoritmo em perícia judicial tecnológica, sem que as empresas de tecnologia necessitem apresentar abertamente o seu código fonte em perícia judicial, a ponto de exibir todo o seu patrimônio intelectual e patrimonial ao mercado. Nesse sentido o Ministério Público/RJ em produção de provas independentes realizadas pelo seu setor pericial as práticas de geo-piercing e geo-blocking pela empresa Decolar.co, simulando em base de dados fictícias as contratações, como se realizadas em diferentes localidades, para atentar o comportamento dos algoritmos nas compras online a depender de onde reside o consumidor, demonstrando a manipulação da base de dados, sem discutir a programação algorítmica em si, afastando-se a discussão em torna da violação da propriedade intelectual. (NETTO; ROSENVALD, 2024, p. 30)

Outro caso que demonstra a possibilidade de se auditar sem infringir a proteção ao segredo industrial trata-se do recurso em Mandado de Segurança em que o STJ[118], através do

jurídica da ação. A ação civil pública é um instrumento jurídico de grande relevância para a proteção dos direitos coletivos e difusos, como os direitos dos consumidores. No contexto do comércio eletrônico, onde as práticas comerciais podem afetar um número significativo de consumidores simultaneamente, este tipo de ação se mostra particularmente eficaz. Este caso específico contra a "Decolar.com" revela a crescente atenção do Ministério Público às práticas comerciais no ambiente digital, especialmente no setor de turismo e viagens online. As plataformas de reservas de hospedagem e passagens aéreas têm sido objeto de escrutínio devido a questões como transparência nos preços, práticas de geolocalização para diferenciação de ofertas, e potenciais violações ao Código de Defesa do Consumidor. A atuação conjunta dos Promotores de Justiça Dr. Guilherme Magalhães Martins e Dr. Pedro Rubim Borges Fortes demonstra a importância da especialização e da colaboração dentro do Ministério Público para lidar com casos complexos que envolvem tecnologia e direito do consumidor. Essa abordagem multidisciplinar é essencial para enfrentar os desafios apresentados pela economia digital em constante evolução. Além disso, este caso serve como um importante precedente para futuras ações relacionadas ao comércio eletrônico, estabelecendo parâmetros para a análise de práticas comerciais online e reforçando a necessidade de as empresas adotarem políticas transparentes e éticas em suas operações digitais. Em suma, o caso contra a "Decolar.com" não apenas destaca a vigilância ativa do Ministério Público na proteção dos direitos dos consumidores no ambiente digital, mas também sinaliza para as empresas do setor a importância de alinharem suas práticas comerciais com as normas de proteção ao consumidor, mesmo – e especialmente – no dinâmico e muitas vezes nebuloso contexto do comércio eletrônico. (FORTES; MARTINS; OLIVEIRA, 2019; MARTINS, 2019; MORASSUTTI, 2019; FALEIROS JÚNIOR; BASAN, 2020).

[118] Eis a ementa: “Recurso ordinário em mandado de segurança. ação civil pública. decretação de segredo de justiça. ilegalidade. existência. geodiscriminação. *geo-pricing*. *geo-blocking*. processo coletivo. publicidade. necessidade, com resguardo apenas dos direitos de propriedade intelectual. 1. As práticas de “geodiscriminação” - discriminação geográfica de consumidores -, como o *geo-pricing* e o *geo-blocking*, desenvolvem-se no contexto da sociedade de risco e da informação, por intermédio de algoritmos computacionais, e - se comprovados - possuem a potencialidade de causar danos a número incalculável de consumidores, em ofensa ao livre mercado e à ordem econômica. 2. O processo coletivo, instrumento

Ministro Luís Felipe Salomão, entendeu que o sigilo excepcionalmente deve imperar no ato processual pericial, isto é, "mantém-se o processo judicial acessível ao público, mas se atribui o sigilo ao ato pericial para impedir que se escancare ao público detalhes técnicos sobre o código-fonte do algoritmo" (FALEIROS, MEDON, 2021, p. 957).

Neste ponto, é importante compreender as estruturas organizacionais e mercadológicas que desenvolvem e comercializam os algoritmos, há quem investe, quem desenvolve, quem coloca no mercado. Por esta razão, os autores Nelson Rosenvald e Felipe Braga entendem que formulam perguntas que levam ao conceito de supervisão (*oversight*[119]), um componente de governança que permite verificações e controles em um processo, mesmo quando o comportamento desejável não pode ser especificado antecipadamente:

> Para estabelecer a relação de explicabilidade, quais agentes são responsáveis por quais outros agentes, ou seja, "responsabilidade de quem?" E "responsabilidade para quem", por quais resultados, e para qual proposito? Se compreendermos quem deve responder, porquê e a quem as respostas estão destinam, alcançamos o conceito de supervisão – oversight – um componente de governança em que uma autoridade detém poder especial para revisar evidências de atividades conectá-las às consequências. A supervisão complementa os métodos os métodos regulatórios de governança (accountability), permitindo verificações e controles em um processo, mesmo quando o comportamento desejável não pudesse ser especificado com antecedência, como uma regra. Ao invés, em caráter *ex post*, uma entidade de supervisão pode separar os comportamentos aceitáveis dos inaceitáveis. Aliás, mesmo quando existem regras, o supervisor pode verificar se o processo agiu de forma consistente dentro delas, sopesando as considerações nas circunstâncias específicas do cenário. (NETTO; ROSENVALD *apud* KROLL, 2020, p. 11)

Resta demonstrado que se prioriza a revisão extrajudicial por humanos em decisões produzidas por algoritmos, conforme exposto no GDPR no art. 71[120]. Não se exige uma

---

vocacionado à tutela de situações deste jaez, é moldado pelo princípio da informação e publicidade adequadas (*fair notice*), segundo o qual a existência da ação coletiva deve ser comunicada aos membros do grupo. 3. A publicidade, erigida a norma fundamental pelo novo Código de Processo Civil (Art. 8º), garante transparência e torna efetivo o controle da atividade jurisdicional, motivo pelo qual também representa imperativo constitucional conforme se depreende do *caput* do art. 37 e do inciso IX do art. 93. 4. Não se desconhece que, em hipóteses excepcionais, é possível a decretação de sigilo de processos judiciais, conforme dispõe o art. 189 do CPC/2015. No entanto, na hipótese, tendo em vista os princípios que informam o processo coletivo e as garantias constitucionais e legais que socorrem os consumidores, o que na verdade atende o interesse público ou social é a publicidade do processo, que versa sobre possível prática de "geodiscriminação". 5. Outrossim, conforme requerido pelo próprio Ministério Público do Estado do Rio de Janeiro e com o escopo de, a um só tempo, resguardar o interesse público e preservar direitos de propriedade intelectual, considero razoável a manutenção do segredo de justiça tão somente no que diz respeito ao algoritmo adotado pela Decolar.com Ltda. e à eventual perícia de informática relativa a tal algoritmo em toda a base de dados adotada para a operação do sistema de reservas eletrônicas. 6. Recurso ordinário em mandado de segurança conhecido e parcialmente provido" (BRASIL, 2019).

[119] Em tradução livre, o termo *oversight* significa fiscalização, superintendência, vigilância.

[120] Art. 71. O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento

explicação completa de todo o processo, mas espera-se uma apresentação daquilo que impacta diretamente na ação ou na decisão. A responsabilidade na modalidade *liability* será utilizada como uma segunda camada de proteção, aplicável quando ocorrem "danos em razão de atos ou atividades danosas que vulneram o *profiling* da pessoa ou alcançam situações existenciais" (NETTO; ROSENVALD, 2024, p. 31).

Do ponto de vista ético, os autores ressaltam que "o objeto principal é a explicabilidade como responsabilidade por parte do ser humano desenvolvedor da IA". Quando um agente humano toma uma decisão baseada na recomendação de uma IA sem compreender plenamente o processo, isso gera um problema duplo de responsabilidade: o agente não atua de forma responsável e falha em sua responsabilidade para com o indivíduo afetado pela decisão (NETTO; ROSENVALD, 2024, p. 31).

A *answerability* se entrelaça com a *responsability*, reconhecendo que "a 'pessoa comum' é relativamente ignorante sobre a tecnologia e suas consequências imprevisíveis" (NETTO; ROSENVALD, 2024, p. 32).

Por isso, a explicação do "por quê" deve ser acompanhada de educação e inclusão digital:

> Isso significa que a sociedade merece operadores responsáveis de IA que estejam no controle, capazes e desejosos de comunicar, explicar e dar razões para o que estão fazendo pacientes morais humanos. Isso inclui a obrigação de obter maior consciência

---

eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança. A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas (EUROPA, 2018).

> das consequências imprevisíveis, incluindo como lidam com problemas trágicos. Se a IA não for responsável nesse sentido, ela irá falhar (NETTO; ROSENVALD, 2024, p. 32).

A necessidade de que tenha alguém responsável pela ação da IA impulsiona o que os autores Nelson Rosenvald e Felipe Braga Netto denominaram de '4ª Lei', para o desenvolvimento de IA enfatizando a necessidade de responsabilidade humana sobre as ações do robô. Segundo os autores, embora os campos de aprendizagem de máquina e robótica enfatizem a autonomia da robótica, é fundamental que haja acompanhamento e revisão humana, especialmente quando resultados infringem direitos (NETTO; ROSENVALD, 2024, p. 32).

A análise da relação entre explicabilidade e responsabilidade civil evidencia a necessidade de uma abordagem dual que contemple tanto aspectos preventivos quanto reparatórios. Esta perspectiva é particularmente relevante quando se considera o atual cenário legislativo brasileiro, onde diversas propostas buscam regular o desenvolvimento e uso da IA. Estas iniciativas legislativas, em diferentes estágios de tramitação, refletem uma crescente preocupação com a transparência e explicabilidade dos sistemas automatizados, propondo mecanismos específicos para garantir que decisões algorítmicas sejam compreensíveis e contestáveis. A compreensão destas propostas é fundamental para avaliar como o ordenamento jurídico brasileiro está se adaptando aos desafios impostos pela IA, especialmente no que tange ao direito à explicação.

5.4.5 Propostas legislativas brasileiras sobre o direito à explicação

No cenário legislativo brasileiro, observa-se uma crescente atenção às questões relacionadas à IA, evidenciada pela tramitação de diversos Projetos de Lei no Congresso Nacional que abordam esta temática.

Dentre as propostas legislativas em análise, destaca-se o PL 21/2020 da Câmara dos Deputados, de autoria do Deputado Eduardo Bismarck e relatoria da Deputada Luiza Canziani, que busca estabelecer um marco legal para o desenvolvimento e uso da IA no Brasil.

A ementa descreve como uma norma que estabelecerá "fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da IA no Brasil", centrando a abordagem da IA no ser humano, tal como descrito na justificativa da própria proposta. E para tanto, quanto a explicabilidade, a sua previsão enquadra-se como princípio para o uso responsável da IA no Brasil (art. 6º, IV):

> IV - transparência e explicabilidade: garantia de transparência sobre o uso e funcionamento dos sistemas de IA e de divulgação responsável do conhecimento de IA, observados os segredos comercial e industrial, e de conscientização das partes interessadas sobre suas interações com os sistemas, inclusive no local de trabalho; (BRASIL, 2020)

E interligado com este princípio garante direito de acesso a informações claras sem conflitar com o art. 20 da norma protetiva de dados:

> Art. 7º.
> [...]
> II - acesso a informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo sistema de IA que lhes afetem adversamente, observados os segredos comercial e industrial; e
> III - acesso a informações claras e completas sobre o uso, pelos sistemas, de seus dados sensíveis, conforme disposto no art. 5º, II, da Lei 13.709, de 2018 – Lei Geral de Proteção de Dados.
> § 1º Os direitos previstos neste artigo não prejudicam o disposto no art. 20 da Lei 13.709, de 2018. (BRASIL, 2020)

Outro projeto de relevância é o PL 2338/2023, apresentado pelo Senador Eduardo Gomes (PL-TO), que traz à tona pontos importantes sobre a regulação equilibrada, visando proteger direitos humanos fundamentais e, simultaneamente, fomentar a inovação tecnológica.

Este projeto legislativo também se centra na pessoa humana (art. 2º, I) e no seu libre desenvolvimento da personalidade (art. 2º, III). A explicabilidade é posta como princípio conjuntamente com a transparência, inteligibilidade e auditabilidade: "Art. 3º.[...] VI – transparência, explicabilidade, inteligibilidade e auditabilidade;" (BRASIL, 2023).

Não obstante a regulação da matéria, o PL 2338/2023 tem sido alvo de críticas por parte de especialistas. Bruno Bioni, Mariana Rielli e Rafael Zanatta argumentam que "há retrocessos muito significativos, como em relação às provisões sobre reconhecimento facial, que impõem à sociedade civil já organizada em torno do processo, bem como a todos preocupados com a pauta antirracista, a urgência de posicionamentos contundentes e articulados" (BIONI; RIELLI; ZANARRA, 2024, p.1).

A proposta legislativa em questão tem como cerne a valorização do elemento humano, demonstrando preocupação "com o que há de material por trás das linhas de código de sistemas de IA". Consequentemente, busca-se preservar a estrutura de direitos, com ênfase naqueles que se ramificam do devido processo informacional, conforme estabelecido no julgamento do caso IBGE[121] pelo STF. Estes direitos incluem a não discriminação, transparência, explicação e

[121] ADIs 6387, 6388, 6389,6390 e 6393. Em 2020, o STF suspendeu o compartilhamento de dados de empresas de telefonia fixa e móvel com o IBGE (Fundação Instituto Brasileiro de Geografia e Estatística). Por maioria, o

revisão quando os impactos materiais gerados pelo sistema sejam significativos sobre um indivíduo ou grupo (BIONI; RIELLI; ZANATTA, 2024, p.4).

Merece destaque, ainda, a previsão de avaliação de impacto e a criação de uma base de dados pública sobre os sistemas de IA. Tais medidas visam permitir uma efetiva *accountability* e o escrutínio público sobre os riscos aceitáveis da tecnologia, promovendo assim uma maior transparência e controle social sobre o desenvolvimento e implementação de sistemas de IA.

Em 17 de abril de 2024, o Senado Federal recebeu, oficialmente, o anteprojeto do CC, que objetiva atualizar as regras cíveis com a nova conjuntura social. E por isto, o tema IA recebeu especial atenção em capítulo próprio, "Capitulo VII", dentro do livro VI, dedicado ao "Direito Civil Digital", que prevê a explicabilidade como garantia:

> Art. . O desenvolvimento de sistemas de IA deve respeitar os direitos de personalidade previstos neste Código, garantindo a implementação de sistemas seguros e confiáveis, em benefício da pessoa natural ou jurídica e do desenvolvimento científico e tecnológico, devendo ser garantidos:
> [...]
> II - condições de transparência, auditabilidade, explicabilidade, rastreabilidade, supervisão humana e governança; (BRASIL, 2023, p. 237)

Esta proposta prevê, ainda, o direito à informação e ao acesso sempre que interagirem ou sofrerem danos:

> Art. . Pessoas naturais que interagirem, por meio de interfaces, com sistemas de IA, incorporados ou não em equipamentos, ou que sofrerem danos decorrentes da operação desses sistemas ou equipamentos, têm o direito à informação sobre suas interações com tais sistemas, bem como sobre o modelo geral de funcionamento e critérios para decisão automatizada, quando esta influenciar diretamente no seu acesso ou no exercício de direitos, ou afetar seus interesses econômicos de modo significativo.

O anteprojeto do CC brasileiro demonstra alinhamento com os preceitos estabelecidos pela LGPD especialmente no que tange à salvaguarda do direito à explicação para indivíduos que tenham seus direitos fundamentais e da personalidade afetados pela utilização de sistemas robóticos. Este movimento legislativo evidencia uma tendência crescente de harmonização entre diferentes instrumentos normativos no ordenamento jurídico brasileiro.

As iniciativas legislativas em curso representam um marco significativo na regulamentação da IA no contexto brasileiro, embora também provoquem discussões multifacetadas acerca do necessário equilíbrio entre o desenvolvimento tecnológico e a

---

Tribunal reconheceu a proteção de dados como direito fundamental e explicitou balizas constitucionais mínimas e necessárias para a limitação desse princípio. (STF, 2024).

proteção dos direitos fundamentais. O constante aprimoramento deste arcabouço regulatório demanda uma interlocução permanente entre os diversos atores envolvidos, incluindo legisladores, especialistas em tecnologia, juristas e membros da sociedade civil, visando assegurar a construção de uma legislação consistente e adaptável aos rápidos avanços tecnológicos no campo da IA.

A compreensão deste cenário normativo em evolução serve como fundamento para a análise das formas de se garantir a explicação, tema que será abordado no próximo capítulo. Esta transição natural evidencia a importância de se estabelecer mecanismos concretos para assegurar a efetividade do direito à explicação, considerando tanto os aspectos jurídicos quanto os desafios técnicos inerentes aos sistemas de IA.

6 CONCLUSÃO:

A presente dissertação examinou o direito à explicação como instrumento fundamental para a proteção dos direitos dos titulares de dados no contexto das decisões automatizadas, analisando sua fundamentação legal, alcance e mecanismos de efetivação no ordenamento jurídico brasileiro. A investigação demonstrou que, diante da crescente implementação de sistemas de IA em processos decisórios automatizados, torna-se imperativa a existência de mecanismos que garantam transparência e *accountability* algorítmica.

O estudo do desenvolvimento histórico da proteção de dados no Brasil revelou uma evolução significativa no tratamento jurídico da matéria, desde as primeiras previsões no CDC até a consolidação de um marco regulatório mais abrangente com a LGPD. Verificou-se que o direito à explicação, embora não explicitamente denominado em todas as normas, encontra fundamento em diversos dispositivos legais, configurando-se como uma garantia essencial para a efetivação da autodeterminação informativa.

A análise comparativa entre o modelo europeu (GDPR) e o brasileiro (LGPD) permitiu identificar convergências e particularidades na abordagem regulatória do direito à explicação. Enquanto o GDPR adota uma postura mais prescritiva, a LGPD apresenta uma flexibilidade que, se por um lado permite maior adaptabilidade às rápidas transformações tecnológicas, por outro demanda uma interpretação sistemática e teleológica para sua efetiva implementação.

O exame da jurisprudência, especialmente do caso paradigmático do STJ sobre sistemas de *credit scoring* (REsp nº 1.419.697/RS), demonstrou a evolução do entendimento judicial sobre transparência algorítmica e direito à explicação. Este precedente estabeleceu importantes parâmetros para o equilíbrio entre as necessidades comerciais e a proteção dos direitos dos titulares de dados, antecipando discussões que seriam posteriormente incorporadas pela LGPD.

A investigação sobre os aspectos técnicos da explicabilidade algorítmica revelou que o direito à explicação não se resume à mera disponibilização de códigos-fonte ou fórmulas matemáticas. A efetiva implementação deste direito requer uma abordagem que combine aspectos técnicos, jurídicos e éticos, garantindo explicações compreensíveis e significativas para os titulares de dados.

No âmbito da responsabilidade civil, identificou-se uma necessária evolução dos conceitos tradicionais para abarcar as especificidades das decisões automatizadas. A pesquisa demonstrou que a explicabilidade emerge não apenas como um direito do titular, mas também como um dever do controlador, configurando-se como elemento essencial para a determinação de responsabilidades e para a própria legitimidade dos sistemas automatizados.

Conclui-se que a efetividade do direito à explicação depende da implementação coordenada de medidas técnicas e jurídicas, incluindo o desenvolvimento de sistemas tecnicamente explicáveis, a adoção de práticas de governança adequadas e o estabelecimento de mecanismos regulatórios que equilibrem transparência e inovação. O estudo contribui para o debate sobre a regulação da IA ao propor uma abordagem integrada que reconhece tanto as limitações técnicas quanto as exigências legais e éticas envolvidas na explicabilidade de sistemas automatizados.

As propostas legislativas em curso, como o PL 21/2020 e o PL 2338/2023, bem como o anteprojeto do novo Código Civil, sinalizam uma tendência de fortalecimento do arcabouço normativo relacionado à IA e ao direito à explicação. No entanto, o sucesso dessas iniciativas dependerá de sua capacidade de estabelecer padrões claros de transparência e accountability, sem obstaculizar o desenvolvimento tecnológico.

Por fim, ressalta-se que o direito à explicação, mais do que uma garantia individual, configura-se como um instrumento essencial para a preservação da autonomia e dignidade humana na era digital. Sua efetivação requer um esforço contínuo de adaptação e aprimoramento dos mecanismos jurídicos e técnicos, assegurando que o desenvolvimento tecnológico permaneça a serviço do bem-estar social e do respeito aos direitos fundamentais.

REFERÊNCIAS

ADAMS, John. **Risco**. São Paulo: Senac, 2009.

AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi. **Prediction Machines**: The Simple Economics of Artificial Intelligence. Boston: Harvard Business Review Press, 2017.

AHMAD, Tanveer; ZHANG, Dongdong; HUANG, Chao; ZHANG, Hongcai. Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. Journal of Cleaner Production, v. 289, 2021. Disponível em: <https://doi.org/10.1016/j.jclepro.2021.125834> Acesso em: 24 de set. 2024.

ALGORITMOS e classificação. **Instagram,** [S.l], 2024. Disponível em: <https://creators.instagram.com/grow/algorithms-and-ranking?locale=pt_BR>. Acesso em: 28 out 2024.

ALVES, Marco Antônio Sousa; ANDRADE, Otávio Morato de**. Da "Caixa-Preta" à "Caixa de Vidro"**: O Uso da Explainable Artificial Intelligence (XAI) para Reduzir a Opacidade e Enfrentar o Enviesamento em Modelos Algorítmicos. Direito Público, Brasília, v. 18, n. 100, p. 349-373, out./dez. 2021. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5973>. Acesso em: 14 maio 2024.

AMAZON. **Perguntas Frequentes sobre Alexa e os Dispositivos Alexa**. Disponível em: <https://abrir.link/VCHFe>. Acesso em: 31 out 2024.

ANANNY, Mike; CRAWFORD, Kate. **Seeing without knowing**: Limitations of the transparency ideal and its application to algorithmic accountability. New Media & Society, v. 20, n. 3, p. 973-989, 2018. Disponível em: <https://journals.sagepub.com/doi/10.1177/1461444816676645>. Acesso em: 18 set. 2024.

ANDRADE, Mariana Dionísio et al. **IA para o rastreamento de ações com repercussão geral**: o projeto Victor e a realização do princípio da razoável duração do processo. Revista Eletrônica de Direito Processual, v. 21, n. 1, jan. 2020. Disponível em: <https://doi.org/10.12957/redp.2020.42717>. Acesso em: 11 set. 2024.

ARBULU, Rafael. **IBM e Microsoft assinam "juramento ético da IA" no Vaticano.** Canaltech, 06 mar. 2020.Disponível em: <https://canaltech.com.br/inteligencia-artificial/ibm-e-microsoft-assinam-juramento-etico-da-inteligencia-artificial-no-vaticano-161188/>. Acesso em: 13 out. 2024.

ARENS, Bob. **Cognitive computing:** under the hood. Thomson Reuters, *[S.l]*, jan. 2017.

ARISTÓTELES. Dos argumentos sofísticos. In: ARISTÓTELES. **Os Pensadores**. São Paulo: Abril, 1973.

ARISTÓTELES. **Política.** Edição Bilíngue. Lisboa: Veja, 1998.

ARTEAGA, Cristian. **Interpretable machine learning for image classification with LIME**: increase confidence in your machine learning model by understanding its prediction. Towards

Data Science, 21 out. 2019. Disponível em: <https://towardsdatascience.com/interpretable-machine-learning-for-image-classification-with-lime-ea947e82ca13>.. Acesso em: 19 set. 2024.

ASIMOV, Isaac. **Eu, Robô**. 1. ed. São Paulo: Aleph, 2014.

ATZ, Ana. Tort Law e Responsabilidade do Produto nos Estados Unidos. In: ATZ, Ana. **Responsabilidade do Produto Tóxico**: O direito e a ciência na Proteção do Consumidor. São Paulo: Revista dos Tribunais, 2022. Disponível em: <https://www.jusbrasil.com.br/doutrina/secao/151-defeito-de-fabricacao-15-acao-de-responsabilidade-do-produto-nos-estados-unidos-elementos-caracterizadores-e-as-especies-de-defeito/1712827644>. Acesso em: 12 out. 2024.

AUGUSTO, Luís Gustavo Henrique; RIZZARDI, Maira Martinelli. Accountability segundo os Ministros dos Tribunais Superiores do Judiciário Brasileiro. In: ENCONTRO NACIONAL DO CONPEDI - DIREITO E ADMINISTRAÇÃO PÚBLICA, 23., 2014, Florianópolis. **Anai**s [...]. Disponível em: <https://www.researchgate.net/publication/280626416_Accountability_segundo_os_Ministros_dos_Tribunais_Superiores_do_Judiciario_Brasileiro_Accountability_according_to_the_Ministers_of_the_Superior_Courts_of_the_Brazilian_Judiciary>. Acesso em: 02 maio 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta**. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta>. Acesso em: 30 out 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Lei Geral de Proteção de Dados Pessoais:** perguntas frequentes. 2024. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes/perguntas-frequentes/1-lei-geral-de-protecao-de-dados-pessoais-lgpd/1-3-quando-a-lgpd>. Acesso em: 14 set. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Relatório de Impacto à Proteção de Dados Pessoais (RIPD**). 2024. Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd>. Acesso em: 26 set. 2024.

BAPTISTA, Rodrigo. Relatório Final dos trabalhos da Comissão de Juristas responsável pela revisão e atualização do Código Civil. Senado notícias, Brasília, 17 abr. 2024. Disponível em: <https://www12.senado.leg.br/noticias/materias/2024/04/17/novo-codigo-civil-senado-recebe-anteprojeto-de-juristas-e-analisara-o-texto>. Senado Federal. Acesso em: 11 de nov de 2024.

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. **Civilista.com**, Rio de Janeiro, a. 3, n. 2, jul./dez. 2014. Disponível em: <https://civilistica.emnuvens.com.br/redc/article/view/151/119>. Acesso em: 02 jul. 2024.

BAUMAN, Zygmunt. **Medo líquido**. Rio de Janeiro: Zahar, 2008.

BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. 2. ed. Tradução: Sebastião Nascimento. São Paulo: Editora 34, 2011.

BELCHIOR, Wilson Sales. IA, princípios e recomendações da OCDE. **Migalhas**, 2024. Disponível em: <https://www.migalhas.com.br/depeso/330983/inteligencia-artificial--principios-e-recomendacoes-da-ocde>. Acesso em: 13 out. 2024.

BENENSON, F. **Whatis Math Washing**. 2021. Disponível em: <https://www.mathwashing.com/>. Acesso em: 20 abril 2024

BENIGER, James R. **The control revolution:** technological and economic origins of the information society. Cambridge: Harvard University Press, 1986.

BESSA, Leonardo; FAIAD, Walter Moura. **Manual de Direito do Consumidor**. Brasília: Ministério da Justiça: Secretaria Nacional do Consumidor, 2014.

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

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação da IA: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, Ana; MOULHOLLAND, Caiti (coord.). **IA e direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019. p. 208-231.

BIONI, Bruno; MONTEIRO, Renato Leite; OLIVEIRA, Maria Cecília. **GDPR Matchup**: Brazil's General Data Protection LAW. IAPP, 4 out. 2018.

BIONI, Bruno; RIELLI, Mariana; ZANATTA, Rafael A. F. **Regulação de IA no Brasil**: Onde estávamos, onde estamos e onde podemos estar. DataPrivacy BR, 30 abr. 2024. Disponível em: <https://www.dataprivacybr.org/regulacao-de-ia-no-brasil-onde-estavamos-onde-estamos-e-onde-podemos-estar/>. Acesso em: 17 jun. 2024.

BLUM, Renato M. S. Opice. **GDPR – General Data Protection Regulation**: destaques da regra europeia e seus reflexos no Brasil. Revista dos Tribunais, São Paulo, v. 107, n. 994, p. 205-221, ago. 2018.

BLUM, Renato Opice. O marco civil da internet e a educação digital no Brasil. In: ABRUSIO, Juliana (coord.). **Educação Digital**. São Paulo: Revistas dos Tribunais, 2015. p. 189-190.

BOHLENDER, Dimitri; KÖHL, Maximilian A. **Towards a Characterization of Explainable Systems**. arXiv:1902.03096 [cs.AI], 31 jan. 2019. Disponível em: <https://doi.org/10.48550/arXiv.1902.03096>. Acesso em: 27 jun. 2024.

BRADFORD, Anu. **The Brussels Effect**: How the European Union Rules the World. New York: Columbia Law School, 2020.

BRANDÃO, Rafael.; *et.al.* **Mediation challenges and socio-technical gaps for explainable deep learning application** [S. l]: [s. n.], 2021.

BRANDEIS, Louis D.; WARREN, Samuel D. **O Direito à Privacidade**. Tradução: Maria Clara de Souza Seixas e Marcus Seixas Souza. Revista de Direito Civil Contemporâneo, São Paulo, v. 38, 2024.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 21/2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e aplicação da inteligência artificial no Brasil. Brasília, 2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340>. Acesso em: 28 out. 2024.

BRASIL. [Lei do Cadastro Positivo] Lei nº 12.414, de 9 de junho de 2011. **Diário Oficial da União**, Brasília, 10 jun. 2011.

BRASIL. Lei nº 12.925, de 26 de dezembro de 2013. Dispõe sobre a criação de cargos de provimento efetivo no Quadro de Pessoal da Secretaria do Tribunal Regional do Trabalho da 22ª Região. **Diário Oficial da União**, Brasília, DF, 27 dez. 2013. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12925.htm>. Acesso em: 27 ago. 2024.

BRASIL. Lei nº 13.853, de 8 de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais. **Diário Oficial da União**, Brasília, DF, 9 jul. 2019.

BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. **Diário Oficial da União**, Brasília, DF, 17 abr. 2020. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Mpv/mpv954.htm>. Acesso em: 27 out 2024.

BRASIL. **Mensagem de Veto nº 288**. Brasília: Senado Federal, 08 jul. de 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm>. Acesso em: 27 ago. 2024.

BRASIL. Lei Nº 9.609, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País e dá outras providências. **Diário Oficial da União**, Brasília, DF, 19 fev. 1998. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9609.htm>. Acesso em: 27 ago. 2024.

BRASIL. Lei Nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 14 ago. 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 27 ago. 2024.

BRASIL. Constituição da República Federativa do Brasil. **Diário Oficial da União**, Brasília, DF, 05 out. 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 27 ago. 2024.

BRASIL. Emenda Constitucional Nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**, Brasília, DF, 10 fev. 2022. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais>. Acesso em: 05 set 2024

BRASIL. Superior Tribunal de Justiça. RECURSO ESPECIAL Nº 1.419.697 - RS (2013/0386285-0). Recurso especial representativo de controvérsia (art. 543-c do cpc). tema 710/stj. direito do consumidor. arquivos de crédito. sistema "credit scoring". compatibilidade com o direito brasileiro. limites. dano moral. Relator: Ministro Paulo de Tarso Sanseverino, 12 de novembro de 2014. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=RECURSO+ESPECIAL+N%C2%BA+1.419.697&O=JT>. Acesso em: 08 de ago. 2024.

BRASIL. Superior Tribunal de Justiça. Recurso Especial Nº 1.418.771 - DF (2013/0382332-9). Recurso especial. Direito civil e processual civil. Ratificação de apelação interposta antes da rejeição dos embargos de declaração. Desnecessidade. Transação para liquidação de sentença coletiva. Legitimidade da associação para pactuação da avença. Existência. Homologação. Juízo de delibação. Coisa julgada. Inexistência. Ausência de vícios no negócio jurídico. Ato jurídico perfeito. Cláusula geral de quitação. Vindicação de verba suplementar em ação condenatória. Inadmissibilidade da via processual eleita e violação da boa-fé objetiva. Constatação. Recorrente : Associacao Nacional Dos Servidores Publicos, Da Previdencia E Da Seguridade Social - Anasps E Outros. Recorrido: GEAP Autogestao Em Saude. Relator Min. Luis Felipe Salomão, 10 de dezembro de 2019. Disponível em: <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201303823329&dt_publicacao=09/09/202>. Acesso em: 14 out. 2024

BROUSSARD, Meredith. **Artificial Unintelligence**: How Computers Misunderstand the World. Cambridge: MIT Press, 2019.

BÜCHI, Moritz et al. **The chilling effects of algorithmic profiling**: Mapping the issues. Computer Law & Security Review, v. 36, p. 105367, 2020. Disponível em: <https://doi.org/10.1016/j.clsr.2019.105367>.Acesso em: 11 set. 2024.

BURRELL, Jenna. **How the machine thinks**: Understanding opacity in machine learning algorithms. Big Data & Society, v. 3, n. 1, jan. 2016. Disponível em: <https://journals.sagepub.com/doi/pdf/10.1177/2053951715622512>. Acesso em: 29 out. 2024.

CABRAL, Julio. **O que é ADAS e como funcionam as tecnologias que evitam acidentes**. Quatro Rodas, 2024. Disponível em: <https://quatrorodas.abril.com.br/noticias/o-que-e-adas-e-como-a-tecnologia-poupa-voce-de-acidentes>. Acesso em: 10 set. 2024.

CALO, Ryan. **Robotics and the Lessons of Cyberlaw.** California Law Review, v. 103, n. 3, p. 513-564, 2015. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2402972>. Acesso em: 17 set. 2024.

CAMPOS, Elisianne. **Ciberespaço, vigilância e privacidade**: o caso google street view. Disponível em: <https://www.academia.edu/1609292/ciberespaco_vigilancia_e_privacidade_o_caso_google_street_view>. Acesso em: 20 jun. 2024.

CARDOSO, Bruno. **Por que fazer uma sociologia da internet?** Sobre o caso Cambridge Analytica e Facebook. Blog do LED-UFRJ, 25 mar. 2018. Disponível em: <https://ledufrj.wixsite.com/ledufrj/post/2018/03/25/por-que-fazer-uma-sociologia-da-internet-sobre-o-caso-cambridge-analytica-e-facebook>. Acesso em: 19 out. 2024.

CARNEIRO, Alvaro Leandro Cavalcante. **Algoritmos de otimização**: Hill Climbing e Simulated Annealing. Medium, 2024. Disponível em: <https://medium.com/data-hackers/algoritmos-de-otimiza%C3%A7%C3%A3o-hill-climbing-e-simulated-annealing-3803061f66f0>. Acesso em: 10 set. 2024.

CASEY, Bryan; FARHANGI, Ashkon; VOGL, Roland. **Rethinking Explainable Machines**: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise. Berkeley Technology Law Journal, v. 34, 2019. Disponível em: <https://ssrn.com/abstract=3143325>. Acesso em: 15 mar. 2024.

CASTELLS, M. **A sociedade em rede**. 6. ed. São Paulo: Paz e Terra, 1999.

CASTOLDI, Augusto Cesar; SANTOS, Marcos de Oliveira dos. **Raciocínio Baseado em Casos**. 2002. Disponível em: <Chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.inf.ufsc.br/~j.barreto/trabaluno/IA20022AugMarc.pdf>. Acesso em: 08 set 2024.

CITRON, Danielle Keats; PASQUALE, Frank. **The Scored Society**: Due Process for Automated Predictions. Washington Law Review, v. 89, 2014. Disponível em: <http://ssrn.com/abstract=2376209>. Acesso em: 10 jul. 2020.

CLANCEY, William; SHORTLIFFE, Edward (org.). **Readings in medical artificial intelligence:** the first decade. Reading: Addison Wesley, 1984.

CLUSTERIZAÇÃO: o que é, como funciona, vantagens algoritmos e quando usar. **TOTVS,** [S.l], 2024. Disponível em: <https://www.totvs.com/blog/inteligencia-de-dados/clusterizacao/>. Acesso em: 13 out. 2024.

COECKELBERGH, Mark. **Artificial Intelligence, responsability attribution, and a relational justification of explainability.** Science and Engineering Ethics, v. 26, p. 2051-2068, ago. 2020. Disponível em: <https://link.springer.com/article/10.1007/s11948-019-00146-8>. Acesso em: 24 jul. 2024.

COHEN, Julie E. **Examined lives:** informational privacy ant the subject as object. Stanford Law Review, v. 52, p. 1373-1438, 2000. Disponível em: <https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?params=/context/facpub/article/1819/&path_info=examined.pdf>. Acesso em: 23 set. 2024.

COMISSÃO EUROPEIA. **A definition of AI**: Main capabilities and scientific disciplines.2019b. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/ethicsguidelines->. Acesso em: 19 ago. 24.

COPPIN, Ben. **Artificial Intelligence Illuminated**. Massachusetts: Jones & Bartlett Learning, 2004.

CORDEIRO, A. Barreto Menezes. Decisões individuais automatizadas à luz do RGPD e da LGPD. In: BARBOSA, Mafalda Miranda et al. Direito **Digital e IA**: diálogos entre Brasil e Europa. Indaiatuba: Foco, 2021.

CORDEIRO, A. Barreto Menezes. **Direito da proteção de dados**. Coimbra: Almedina, 2020, p. 326-335 e 346-347.

CORTIZ, Diogo. IA: conceitos fundamentais. In: VAINZOF, Rony; GUTIERREZ, Andrei (org.). **IA: sociedade, economia e Estado**. São Paulo: Thomson Reuters, 2021. p. 45-60.

COSTA, Ramon Silva; DE OLIVEIRA, Samuel Rodrigues; NEGRI, Sergio Marcos Carvalho de Ávila. **O uso de tecnologias de reconhecimento facial baseadas em IA e o direito à proteção de dados.** Direito Público, *[S. l.]*, v. 17, n. 93, 2020. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3740>. Acesso em: 1 jun. 2024.

DE GIORGI, Raffaele. O direito na sociedade do risco. **Revista Opinião Jurídica**, Fortaleza, v. 3, n. 5, p. 383-394, 2005. DOI: 10.12662/2447-6641oj.v3i5.p383-394.2005. Disponível em: <https://periodicos.unichristus.edu.br/opiniaojuridica/article/view/2866>. Acesso em: 02 maio 2024.

DE LUCCA, Newton. A proteção dos consumidores no âmbito da internet. In: LIMA, Cíntia Rosa Pereira de; NUNES, Lydia Neves Bastos Telles (coord.). **Estudos avançados de direito digital**. São Paulo: Elsevier, 2014. p. 97.

DENSA, Roberta; DANTAS, Cecília. Notas sobre publicidade digital: cookies e spams. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (coord.). **Direito digital:** direito privado e Internet. 4. ed. São Paulo: Foco, 2021. p. 694-700.

DIAS, Tatiana. Não cadastre biometria na Droga Raia. **O Intercept Brasil,** [S.l], 05 jul, 2021. Disponível em: <https://www.intercept.com.br/2021/07/05/nao-cadastre-biometria-na-droga-raia/>. Acesso em: 18 jun. 2024.

DONEDA, Danilo Cesar Maganhoto et al. Considerações iniciais sobre IA, ética e autonomia pessoal. **Pensar**, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018. Disponível em: <https://ojs.unifor.br/rpen/article/view/8257>. Acesso em: 26 set. 2024.

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

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021.

DORAN, Derek; SCHULZ, Sarah; BESOLD, Tarek. What does explainable AI really mean? A new conceptualization of perspectives. In: INTERNATIONAL WORKSHOP ON COMPREHENSIBILITY AND EXPLANATION IN AI AND ML, 1., 2017. **Proceedings** [...]. arXiv:1710.00794, 2017.

DOSHI-VELEZ, Finale; KORTZ, Mason. **Accountability of AI Under the Law:** The Role of Explanation. Berkman Klein Center Working Group on Explanation and the Law, 2017. Disponível em: <https://dash.harvard.edu/handle/1/34372584>. Acesso em: 05 maio 2024.

DREHMER, Vitória. Carro autônomo do Google está sob investigação após incidentes nos EUA. [s.l]: **Autoesporte**, 20 maio 2024. Disponível em: <https://autoesporte.globo.com/setor-automotivo/transportes-publicos-e-alternativos-mobilidade/noticia/2024/05/carro-autonomo-do-google-esta-sob-investigacao-apos-incidentes-nos-eua.ghtml>. Acesso em: 11 set. 2024.

DROGA RAIA. **Política de Privacidade**. 2020. Disponível em: <https://web.archive.org/web/20200919052054/https://www.drogaraia.com.br/politica-de-privacidade>. Acesso em: 18 jun. 2024.

EM 2022, expectativa de vida era de 75,5 anos**.** Rio de Janeiro: **Instituto Brasileiro de Geografia e Estatística,** 29 nov. 2023. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/38455-em-2022-expectativa-de-vida-era-de-75-5-anos>. Acesso em: 15 set. 2024.

ÉPOCA NEGÓCIOS. Amazon desiste de ferramenta secreta de recrutamento que mostrou viés contra mulheres. 2018. Disponível em: <https://epocanegocios.globo.com/Empresa/noticia/2018/10/amazon-desiste-de-ferramenta-secreta-de-recrutamento-que-mostrou-vies-contra-mulheres.html>. Acesso em: 15 maio 2024.

ETIQUETA (metadados). Wikipedia, [S.l], 25 ago. 2019. Disponível em: <https://pt.wikipedia.org/wiki/Etiqueta_(metadados)#:~:text=Uma%20tag%2C%20ou%20em%20portugu%C3%AAs,informa%C3%A7%C3%A3o%20baseada%20em%20palavras%2Dchave.&text=Tags%20ou%20etiquetas%20s%C3%A3o%2C%20usualmente,ou%20etiquetas%20associadas%20a%20ele.>. Acesso em: 05 de maio de 2024.

EUROPE. (GDPR) Regulamento Geral de Proteção de Dados. Intersoft Consulting, [S.l], 05 maio, 2018. Disponível em:<https://gdpr-info.eu/art-99-gdpr/>. Acesso em: 04 set. 2024.

EUROPEAN DATA PROTECTION BOARD. **About EDPB**. Disponível em: <https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en>. Acesso em: 20 jul 2024.

EUROPEAN COMMISSION. Artificial Intelligence Robotics and ‘Autonomous’ Systems. Disponível em: <https://www.academia.edu/85790742/Artificial_Intelligence_Robotics_and_Autonomous_Systems_Statement_on_EUROPEAN_COMMISSION_Directorate_General_for_Research_and_Innovation_2018_Statement_on_Artificial_Intelligence_Robotics_and_Autonomous_Systems>. Acesso em: 13 out 2024.

EUROPEAN DATA PROTECTION BOARD. O Conselho Europeu para a Proteção de Dados. [S.l], 06 abr. 2022. Disponível em: <https://edpb.europa.eu/about-edpb/about-edpb_en> .Acesso em: 04 set 2024.

EXPLAINABLE AI. **IBM**, [s.l], 2024. Disponível em: <https://www.ibm.com/br-pt/topics/explainable-ai>. Acesso em: 28 out 2024.

FALEIROS JÚNIOR, José Luiz de Moura; MEDON, Filipe. Discriminação algorítmica de preços, perfilização e responsabilidade civil nas relações de consumo. **Revista de Direito da Responsabilidade**, ano 3, p. 947-969, 2021. Disponível em: <https://revistadireitoresponsabilidade.pt/2021/discriminacao-algoritmica-de-precos-perfilizacao-e-responsabilidade-civil-nas-relacoes-de-consumo-jose-luiz-de-moura-faleiros-junior-filipe-medon>. Acesso em: 07 out. 2024.

FALEIROS JÚNIOR , José Luiz de Moura; BASAN, Arthur Pinheiro. Desafios da predição algorítmica na tutela jurídica dos contratos eletrônicos de consumo. **Revista da Faculdade de Direito da UFRGS**, n. 44, 131-153, dez. 2020.

FANTÁSTICO. Medo, frustrado e constrangido, diz homem detido por engano em estádio após erro do sistema de reconhecimento facial. **G1**, 21 abr. 2024. Disponível em: <https://g1.globo.com/fantastico/noticia/2024/04/21/medo-frustrado-e-constrangido-diz-homem-detido-por-engano-em-estadio-apos-erro-do-sistema-de-reconhecimento-facial.ghtml>. Acesso em: 22 abr. 2024.

FERRARI, Isabela. Accountability de Algoritmos: a falácia do acesso ao código e caminhos para uma explicabilidade efetiva. **Artigos abertos**: IA, Rio de Janeiro, mar. 2019. Disponível em: <https://itsrio.org/pt/publicacoes/inteligencia-artificial-gp3/>. Acesso em: 1 dez. 2023.

FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. Arbitrium ex machina: panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. **Revista dos Tribunais**, São Paulo, n. 995, set. 2018.

FINK, Varda N. Consumer Protection: Regulation and Liability of the Credit Reporting Industry. **Notre Dame Law**, v. 47, p. 1291, 1971.

FLORIDI, Luciano. Soft ethics, the Governance of the digital and the General Data Protection Regulation. **Philosophical Transactions of the Royal Society A**, 2018. Disponível em: <https://royalsocietypublishing.org/doi/10.1098/rsta.2018.0081>. Acesso em: 01 jul. 2024.

FLORIDI, Luciano; COWLS, Josh. A Unified Framework of Five Principles for AI in Society. **Harvard Data Science Review**, v. 1, n. 1, jun. 2019. DOI: 10.1162/99608f92.8cd550d1. Disponível em: <https://hdsr.mitpress.mit.edu/pub/l0jsh9d1/release/8>. Acesso em: 20 abr. 2024.

FORTES, Pedro Rubim Borges; MARTINS, Guilherme Magalhães; OLIVEIRA, Pedro Farias. O consumidor contemporâneo no Show de Truman: a geodiscriminação digital como prática ilícita no direito brasileiro. **Revista de Direito do Consumidor**, n. 124, 235-260, jul./ago. 2019

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. 14. ed. Petrópolis: Vozes, 1996.

FRAJHOF, Isabella Z. O papel dos mecanismos de compliance para a operacionalização do direito à explicação de decisões totalmente automatizadas. In: FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (org.). **Compliance e Políticas de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 467-494.

FRAZÃO, Ana. Controvérsias em torno do direito à explicação e à oposição diante de decisões totalmente automatizadas. **Revista JOTA**, 12 dez. 2018. Disponível em < https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/controversias-sobre-direito-a-explicacao-e-a-oposicao-diante-de-decisoes-automatizadas >. Acesso em 01 set 2024.

FRAZÃO, Ana. O direito à explicação e à oposição diante de decisões totalmente automatizadas. **Revista JOTA**, 5 dez. 2018. Disponível em <shorturl.at/epAH7> Acesso em 18 set 2024.

FRAZÃO, Ana; GOETTENAUER, Carlos. O jogo da imitação jurídica: o direito à revisão de decisões algorítmicas como um mecanismo para a necessária conciliação entre linguagem natural e infraestrutura matemática. In: TEPEDINO, Gustavo; SILVA, Rodrigo da Guia (org.). **O Direito Civil na era da IA**. São Paulo: Thomson Reuters Brasil, 2020. p. 45-64.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Viviane da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **A Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato. **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. E-book Kindle.

FREIRE, Paulo. **Educação como Prática da Liberdade**. 26. ed. Rio de Janeiro: Paz e Terra, 2002.

FROOMKIN, A. Michael. The death of privacy? **Stanford Law Review**, v. 32, p. 1461-1544, 2000.

GALGANO, Francesco. **Lex mercatoria**. 5. ed. Bologna: Il Mulino, 2010.

GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. **Computer Law & Security Review**: The International Journal of Technology Law and Practice, 2017. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364917302698>. Acesso em: 02 out. 2024.

GOETTENAUER, Carlos Eduardo. Algoritmos, IA, mercados: desafios ao arcabouço jurídico. In: FRAZÃO, Ana; CARVALHO, Angelo Gamba Prata de (coord.). **Empresa, mercado e tecnologia**. Belo Horizonte: Fórum, 2019. p. 271-274.

GOMES, Luiz Flávio. Normas justificantes e normas permissivas. **Migalhas**, 16 mar., 2007. Disponível em: <https://www.migalhas.com.br/depeso/36817/normas-justificantes-e-normas-permissiva>. Acesso em: 14 set. 2024.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados pessoais: uma breve análise da sua definição e papel na LGPD. **Revista do Advogado**, n. 144, p. 6-15, 2019.

GOMEZ, Vitoria Lopes. Nova IA pode prever tendências do mercado de ações. **Olhar** Digital, [S.l], 24 nov. 2023. Disponível em: <https://olhardigital.com.br/2023/11/24/pro/quer-investir-sem-risco-nova-ia-pode-prever-tendencias-do-mercado-de-acoes/>. Acesso em: 09 set. 2024.

GONÇALVES, Bernardo; SOUZA, Clarisse de; CARBONERA, Joel. O problema da explicação em IA: considerações a partir da semiótica**. Teccogs**: Revista Digital de Tecnologias Cognitivas, São Paulo, n. 17, p. 59-75, jan./jun. 2018. Disponível em: <https://revistas.pucsp.br/index.php/teccogs/article/view/48590>. Acesso em: 27 out. 2024.

GOODMAN, Bryce; FLAXMAN, Seth. EU Regulations on Algorithmic Decision Making and "a Right to an Explanation". In: ICML WORKSHOP ON HUMAN INTERPRETABILITY IN ML (WHI), 2016, Nova Iorque. **Anais** [...]. Disponível em: <https://arxiv.org/abs/1606.08813>. Acesso em: 18 fev. 2024.

GOUVEIA, Aline. 11 de Setembro: após 22 anos, relembre o atentado às Torres Gêmeas. **Estados Unidos**, [*S. l.*], p. 1 - 10, 11 set. 2023. Disponível em: https://www.correiobraziliense.com.br/mundo/2023/09/5124353-11-de-setembro-apos-22-anos-relembre-o-atentado-as-torres-gemeas.html#google_vignette. Acesso em: 22 mar. 2024

GRINT, Keith.; WOOLGAR, Steve. **The Machine at Work**: technology, work and organization. 2013.

GRUPO DE TRABALHO DO ARTIGO 29. **Guidelines for identifying a controller or processor's lead supervisory authority**. 13 dez. 2016. Disponível em: <http://ec.europa.eu/newsroom/document.cfm?doc_id=44102>. Acesso em: 19 set. 2024.

GRUPO DE TRABALHO DO ARTIGO 29. **Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679**. 2017. Disponível em: <http://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=612053>. Acesso em: 11 abr. 2024.

GRUPO DE TRABALHO DO ARTIGO 29**. Guidelines on Data Protection Impact Assessment (DPIA).** 04 abr. 2017. Disponível em: <http://ec.europa.eu/newsroom/document.cfm?doc_id=44137>. Acesso em: 19 set. 2024.

GRUPO DE TRABALHO DO ARTIGO 29. **Guidelines on the right to data portability**. 2016. Disponível em: <https://ec.europa.eu/newsroom/article29/items/611233>. Acesso em: 19 set. 2024.

GUNZI, Arnaldo. Husky ou lobo?. **Ideias Esquecidas**, São Paulo, 2020. Disponível em: <https://ideiasesquecidas.com/2020/05/19/husky-ou-lobo/>. Acesso em: 29 abr. 2024.

HAN, Byung-Chul. **No enxame**: perspectivas do digital. Tradução: Lucas Machado. Petrópolis: Vozes, 2018.

HAN, Byung-Chul. **Psicopolítica**: o neoliberalismo e as novas técnicas de poder. Tradução: Maurício Leisen. Belo Horizonte: Âyiné, 2018.

HARARI, Yuval Noah. **21 lições para o século 21**. Tradução: Paulo Geiger. São Paulo: Companhia das Letras, 2018.

HARPER, Jim. Reputation Under Regulation: the Fair Credit Reporting Act at 40 and lessons for the Internet privacy debate. **Policy Analysis**, n. 690, dez. 2011.

HAY, Felipe Artigas. IA e princípios de Asilomar. **Revista Teste**, v. 1, n. 2, 2024. Disponível em: <https://revista.unicuritiba.edu.br/index.php/revteste/article/view/6611>. Acesso em: 13 out. 2024.

HEIDEGGER, M. **Einleitung in die Philosophie**. Frankfurt am Main: Vittorio Klostermann, 1996. Tradução de Marco Antônio Casanova. São Paulo: Martins Fontes, 2008.

Helen NISSENBAUM, **Privacy in contex**t: technology, policy, and the integrity of social life, Stanford University Press, 2010, 231

HERN, A. 'Partnership on AI' formed by Google, Facebook, Amazon, IBM and Microsoft. **The Guardian**, 29 jun. 2016. Disponível em: <http://www.theguardian.com/technology/2016/sep/28/google-facebook-amazonibm-microsoft-partnership-on-ai-tech-firms>. Acesso em: 20 mar. 2024.

HIATT, Keith; KLEINMAN, Michael; LATONETO, Mark. Tech folk: "Move fast and break thing" doesn't work when lives are at stake. The Guardian, 2017. Disponível em: <https://www.theguardian.com/global-development-professionalsnetwork/2017/feb/02/technology-human-rights>. Acesso em: 17 set. 2024.

HIDDEN LAYER. **DeepAI**, [S.l.]. Disponível em: <https://www.google.com/search?q=HIDDEN+LAYER.+DeepAI&oq=HIDDEN+LAYER.+DeepAI&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzUzNmowajeoAgCwAgA&sourceid=chrome&ie=UTF-8>. Acesso em: 18 set 2024.

HILDEBRANDT, Mireille. Defining Profiling: A New Type of Knowledge?. In: HILDEBRANDT, Mireille; GUTWIRTH, Serge (org.). **Profiling the European Citizen: Cross-Disciplinary Perspectives**. Dordrecht: Springer Netherlands, 2008. p. 17-45.

HOFFMAN, Robert R. et al. **Explaining Explanation Part 4:** A Deep Dive on Deep Nets. IEEE Intelligent Systems, 2018, v. 33, n. 3, p. 87-95.

IA e uma rede social abandonada: os segredos do Google Fotos. **Olhar digital.** [S.l], 03 nov. 2017. Disponível em: <https://olhardigital.com.br/2017/11/03/noticias/i-a-e-uma-rede-social-abandonada-os-segredos-do-google-fotos/>. Acesso em: 04 jun. 2024.
ICMC-USP. **Genetic Algorithms**. Disponível em: <https://sites.icmc.usp.br/andre/research/genetic/>. Acesso em: 08 set. 2024.

IEEE. IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. [S.l], 2024. Disponível em: <https://standards.ieee.org/industry-connections/activities/ieee-global-initiative/>. Acesso em: 13 out. 2024.

INFANTÁRIO, Juliano. Declaração da Direcção-Geral da Investigação e Inovação da COMISSÃO EUROPEIA sobre a Inteligência Artificial, Robótica e Sistemas "Autónomos" 2018 Declaração da Direcção-Geral da Investigação e Inovação sobre a Inteligência Artificial, Robótica e Sistemas "Autónomos". Artificial Intelligence, Robotics and autonumus systems, [S.l], 2018. <https://www.academia.edu/85790742/Artificial_Intelligence_Robotics_and_Autonomous_Systems_Statement_on_EUROPEAN_COMMISSION_Directorate_General_for_Research_and_Innovation_2018_Statement_on_Artificial_Intelligence_Robotics_and_Autonomous_Systems>. Acesso em 15 out. 2024

KAMINSKI, Margot E. Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability. **Southern California Law Review**, v. 92, n. 6, 2019. Disponível em: <https://scholar.law.colorado.edu/faculty-articles/1265/>. Acesso em: 07 set. 2024.

KAMINSKI, Margot E. The Right to Explanation, Explained. **Berkeley Technology Law Journal**, v. 34, n. 1, 2019. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3196985>. Acesso em: 07 set. 2024.

KITCHIN, Rob. Thinking critically about and researching algorithms. **Information, Communication & Society,** v. 20, n. 1, p. 14-29, 2017. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2515786>. Acesso em: 17 set. 2024.

LEHR, David; OHM, Paul. Playing with the Data: What Legal Scholars Should Learn About Machine Learning. **UC Davis Law Review**, v. 51, p. 653, 2017. Disponível em: <https://lawreview.law.ucdavis.edu/archives/51/2/playing-data-what-legal-scholars-should-learn-about-machine-learning>. Acesso em: 04 ago. 2024.

LESSIG, Lawrence. **Code and Other laws of cybersapace**. New York: Basic Books, 1999.

LIMA, Taisa Maria Macena de. Principiologia sobre IA, Robótica e Sistemas Autônomos. **Virtuajus**, v. 4, n. 7, p. 12-22, 2019. DOI: 10.5752/P.1678-3425.2019v4n7p12-22. Disponível em: <https://periodicos.pucminas.br/index.php/virtuajus/article/view/21927>. Acesso em: 10 fev. 2024.

LIMA, Taisa Maria Macena de. SÁ, Maria de Fátima Freire de. Inteligência Artificial e Lei Geral de Proteção de Dados Pessoais: O Direito à Explicação nas Decisões Automatizadas. **Revista Brasileira de Direito Civil:** [S.l]. v. 26. P. 227-246, out/dez.2020.

LIPOVETSKY, Gilles. **A era do vazio**: ensaios sobre o individualismo contemporâneo. São Paulo: Manole, 2005.

LOBO JUNIOR, Mario Cesar. Privacy by Design e LGPD: Um legado de estudos em privacidade e proteção de dados. **Migalhas**, 25 ago. 2020. Disponível em: <https://www.migalhas.com.br/depeso/332405/privacy-by-design-e-lgpd--um-legado-de-estudos-em-privacidade-e-protecao-de-dados>. Acesso em: 12 out. 2024.

MAGRANI, Eduardo. **A Internet das Coisas**. Rio de Janeiro: FGV, 2018.

MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. **Computer Law & Security Review**, v. 32, n. 2, p. 238-255, 2016.

MARQUES, Claudia Lima. Confiança no comércio eletrônico e a proteção do consumidor: um estudo dos negócios jurídicos de consumo no comércio eletrônico. São Paulo: **Revista dos Tribunais**, 2004.

MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3. ed. São Paulo: Atlas, 2016.

MARTINS, Guilherme Magalhães. O geopricing e geoblocking e seus efeitos nas relações de consumo. In: **IA e direito**: ética, regulação e responsabilidade (coord. Ana Frazão/Caitlin Mulholland), Thomson Reuters Brasil, 2019, 633-650.

MATHWORKS. Machine Learning. [S.l], 2024.Disponível em: <https://www.mathworks.com/discovery/machine-learning.html>. Acesso em: 09 set. 2024.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: A Revolution That Will Transform How We Live, Work, and Think. London: John Murray Publishers, 2013.

MCCARTHY, John. **What is artificial intelligence?** Stanford University, 2007. Disponível em: <https://www.formal.stanford.edu/jmc/whatisai.pdf>. Acesso em: 1 jul. 2024.

MCGONAGLE, Jonh *et al.* **Backpropagation**. Brilliant.org, [S.l], 2024. Disponível em: <https://brilliant.org/wiki/backpropagation/>. Acesso em: 10 set. 2024.

MEDON, Filipe**. IA e responsabilidade civil**: autonomia, riscos e solidariedade. Salvador: Juspodivm, 2020.

MEIRA, Cinthia Gabriele Eufrosina *et al*. **Ícone e símbolo**: a semiótica Peirceana na língua brasileira de sinais. Mimesis, Bauru, 2017, v. 38, n. 2, p. 157-166.

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

MENKE, Fabiano. Migalhas de proteção de dados: as origens alemãs e o significado da autodeterminação informativa. **Migalhas**, 30 out. 2020. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/335735/as-origens-alemas-e-o-significado-da-autodeterminacao-informativa>. Acesso em: 22 jul. 2024.

MICHAELIS. Oligopólio. [S.l], 2024Disponível em: <https://michaelis.uol.com.br/busca?r=0&f=0&t=0&palavra=oligopolio>. Acesso em: 13 out. 2024.

MILHAUPT, Curtis J.; PISTOR, Katharina. **Law and capitalismo: what corporate crises reveal about legais systems and economic developmente around the world**. Chicago: The University of Chicago Press, 2008. Disponível em: <https://edisciplinas.usp.br/pluginfile.php/4093445/mod_resource/content/0/Curtis%20J.%20Milhaupt%2C%20Katharina%20Pistor-

Law%20%20Capitalism_%20What%20Corporate%20Crises%20Reveal%20about%20Legal%20Systems%20and%20Economic%20Development%20around%20the%20World%20%282008%29.pdf>. Acesso em: 23 set. 2024.

MILLER, Arthur R. **Computers, Data Banks and Individual Privacy**: An Overview. Columbia Human Rights Law Review, v. 4, p. 1, 1972.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO. Estratégia Brasileira de Inteligência Artificial. Brasília, 2024. Disponível em: <https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial>. Acesso em: 13 out. 2024.

MITCHELL, Margareth *et.al.* **Model Cards for Model Reporting. FAT* '19**, Atlanta, GA, USA, 2019.

MITTELSTADT, Brent et al. **The Ethics of Algorithms**: Mapping the Debate. Big Data & Society, v. 3, n. 2, 2016. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/2053951716679679>. Acesso em: 17 set. 2024.

MODENESI, Pedro. Contratos eletrônicos de consumo: aspectos doutrinário, legislativo e jurisprudencial. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (coord.). **Direito digital**: direito privado e Internet. 4. ed. São Paulo: Foco, 2021. p. 564.

MOLNAR, Christoph. **Interpretable machine learning**: a Guide for Making Black Box Models Explainable. Leanpub, 2021. Disponível em: <https://christophm.github.io/interpretable-ml-book/>. Acesso em: 20 maio 2024.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Artigo Estratégico**, Rio de Janeiro: Instituto Igarapé, n. 39, dez. 2018. Disponível em: <shorturl.at/dtxU8>. Acesso em: 20 mar. 2023.

MORAIS, Fausto Santos de. **O uso da IA na repercussão geral**: desafios teóricos e éticos. Direito Público, v. 18, n. 100, 2022. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6001>. Acesso em: 23 maio 2024.

MORASSUTTI, Bruno Schimitt. Responsabilidade civil, discriminação ilícita e algoritmos computacionais: breve estudo sobre as práticas de geoblocking e geopricing. **Revista de Direito do Consumidor,** n. 124, p. 213-234, jul./ago. 2019.

MULHOLLAND, Caitlin. A tutela da privacidade na internet das coisas (IOT). In: MAGRINI, Eduardo (org.). **Horizonte presente**: debates de tecnologia e sociedade. Rio de Janeiro: Letramento, 2019. v. 1.

MULHOLLAND, Caitlin. 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**, v. 19, 2018.

MULHOLLAND, Caitlin; FRAJHOF, Isabela Z. IA e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio

de machine learning. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **IA e Direito**: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. IA e a Lei Geral de Proteção de Dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de machine learning. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **IA e Direito**: Ética, Regulação e Responsabilidade. São Paulo: Thomson Reuters, 2019. p. 265-290.

MÜLLER, Klaus-Robert; SAMEK, Wojciech. **Towards explainable artificial intelligence**. Disponível em: <https://arxiv.org/abs/1909.12072>. Acesso em 01 jul 2024.

NABEEL, Fahad. **Regulating facial recognition technology in public places**. Centre for Strategic and Contemporary Research, [S.l], 2019. Disponível em: <https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_Places>. Acesso em: 02 jul. 2024.

NADIN, M. In folly ripe. **In reason rotten**: putting machine theology to rest. [s.l]2017. Disponível em: <https://arxiv.org/abs/1712.04306v1>. Acesso em: 4 maio 2018.

NALIN, Carolina. **Mulheres são minoria em cursos de TI e percentual de formadas em exatas cai em dez anos**. O Globo, 8 mar. 2024. Disponível em: <https://oglobo.globo.com/economia/noticia/2024/03/08/mulheres-sao-minoria-em-cursos-de-ti-e-percentual-de-formadas-em-exatas-cai-em-dez-anos.ghtml>. Acesso em: 29 out. 2024.

NETTO, Felipe Braga; ROSENVALD, Nelson. **Responsabilidade civil:** teoria geeral. Editora Foco: Indaiatuba, 2024.

NISSENBAUM, Helen. **Privacy in context**: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010, p. 289.

NORRIS, Clive. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, David. **Surveillance as social sorting**: privacy, risk, and digital discrimination. New York: Routledge, 2003.

NUNES, Dierle José Coelho; ANDRADE, Otávio Morato de. O uso da IA explicável enquanto ferramenta para compreender decisões automatizadas: possível caminho para aumentar a legitimidade e confiabilidade dos modelos algorítmicos? **Revista Eletrônica do Curso de Direito da UFSM**, v. 18, n. 1, p. e69329, 2023. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/69329>. Acesso em: 24 maio 2024.

OLIVEIRA, Elsa Dias. **A protecção dos consumidores nos contratos celebrados através da Internet**. Coimbra: Almedina, 2002.

OLIVEIRA, R. C. DE A. DE. Produzindo a Vulnerabilidade do Consumidor: Tecnologias Biométricas, Marketing e Biopolítica. **Revista Interdisciplinar de Marketing**, v. 13, n. 1, p. 19-32, 29 jan. 2023. Disponível em: <https://periodicos.uem.br/ojs/index.php/rimar/article/view/66251>. Acesso em: 18 jun. 2024.

O'NEIL, Cathy. **Algoritmos de Destruição em Massa**. São Paulo: Rua do Sabão, 2021.

O'NEIL, Cathy. The era of blind faith in big data must end. **TED**, abr. 2017. Disponível em: <https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end?language=en>. Acesso em: 15 jun. 2024.

OSÓRIO, Fernando. Redes Neurais – Aprendizado Artificial. Fórum de I.A. [s.l], 2024. Disponível em: <osorio.wait4.org/oldsite/IForumIA/fia99.pdf>. Acesso em: 17 set 2024.

PACIFICO, Jonathan. LIME: **Un outil d'interprétabilité des algorithmes de classification**. Avanade, 2024. Disponível em: <https://www.avanade.com/fr-fr/blogs/le-blog/data-and-ia/lime-interpretabilite-algorithmes-classification>. Acesso em: 27 out. 2024.

PACHECO, Rodrigo. **Projeto de Lei nº 2338/2023**. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 03 maio 2023.Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 28 out. 2024.

PARTIDA na Arena Batistão marca nova estratégia de segurança pública com reconhecimento facial. Sergipe,16 fev.2024. Disponível em: <https://www.se.gov.br/noticias/seguranca-publica/partida_na_arena_batistao_marca_nova_estrategia_de_seguranca_publica_com_reconhecimento_facial_para_jogos_do_futebol_sergipano>. Acesso em: 30 mar. 2024.

PEARL, J. **Probabilistic reasoning in intelligent systems**. San Francisco: Morgan Kaufmann, 1988.

PIRES, Thatiane Cristina Fontão; SILVA, Rafael Peteffi da. A responsabilidade civil pelos atos autônomos da IA: notas iniciais sobre a resolução do Parlamento Europeu. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 239-254, dez. 2017. Disponível em: <https://www.publicacoes.uniceub.br/RBPP/article/view/4951>. Acesso em: 19 set. 2024.

PRADO, Adélia. **Bagagem.** São Paulo: Siciliano, 1993.

POLÍTICA de Privacidade. **Google,** [S.l], [20--]. Disponível em: <https://policies.google.com/privacy?hl=pt-BR>. Acesso em 27 out 2024.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. **Law, Innovation and Technology**, v. 10, n. 1, p. 40-81, 2018.

QUEIROZ, Danilo Duarte de. Privacidade na Internet. In: FILHO, Demócrito Reinaldo (coord.). **Direito da Informática**: temas polêmicos. São Paulo: Edipro, 2002. p. 88.

RAIA DROGASIL. **Política de Privacidade LGPD**. [S.l] 2021. Disponível em: <https://web.archive.org/web/20210118041403/https://www.rd.com.br/politicas-lgpd/politica-de-privacidade-canais.pdf>. Acesso em: 18 jun. 2024.

RAMOS, Oscar Garcia. **"Black box":** there's no way to determine how the algorithm came to your decision. Towards Data Science. [S.l], 2024.Disponível em: <https://towardsdatascience.com/black-box-theres-no-way-to-determine-how-the-algorithm-came-to-your-decision-19c9ee185a8>. Acesso em: 25 maio 2024.

REMIGIO, Matheus. Aprendizagem Baseada em Instâncias — KNN. **Medium**, 11 ago.2024. Disponível em: <https://medium.com/@msremigio/aprendizagem-baseada-em-inst%C3%A2ncias-knn-7e2c6f0778bc>. Acesso em: 14 out. 2024.

REVISÃO de desativação. **UBER**, [S.l], 2024. Disponível em: <https://www.uber.com/br/pt-br/drive/driver-app/deactivation-review/>. Acesso em 10 set 2024.

RIBEIRO, Marco Túlio; SINGH, Sammer; GUESTRIN, Carlos. **Why Should I trust you?**: explaining the predictions of any classifier. arXiv:1602.04938 [cs.LG], 16 fev. 2016. Disponível em: <https://arxiv.org/abs/1602.04938>. Acesso em: 25 maio 2024.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. 1. ed. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. Some Remarks on Surveillance Today. **European Journal of Law and Technology**, v. 4, n. 2, 2013. Disponível em: <https://ejlt.org/index.php/ejlt/article/view/277/388>. Acesso em: 02 jun. 2024.

RODRIGUES, Ricardo B. et al. A cloud-based recommendation model. In: Euro American Conference On Telematics And Information Systems, 7., 2014, Valparaíso. **Proceeding**s [...]. 2014.

ROSENVALD, Nelson; OLIVEIRA, Fabrício de Souza. **O ilícito na governança dos grupos de sociedades**. Salvador: Juspodivm, 2019.p. 331.

ROSSETI, Regina; ANGELUCI, Alan. Ética algorítmica: questões e desafios éticos do avanço tecnológico da sociedade da informação. **Galáxia**, n. 46, p. 1-18, 2021. Disponível em: <https://www.scielo.br/j/gal/a/R9F45HyqFZMpQp9BGTfZnyr/?lang=pt>. Acesso em: 24 maio 2024.

ROUVROY, A.; BERNS, T. **Le nouveau pouvoir statistique**. Multitudes, Paris, n. 40, p. 88-103, 2010.

RUSSELL, Stuart J.; NORVIG, Peter. **Artificial Intelligence**: a modern approach. 3. ed. New Jersey: Pearson Education, 2010.

SÁ, Maria da Fátima Freire de; NAVES, Bruno Torquato de Oliveira. **Bioética e Biodireito**. 6. ed. Indaiatuba: Foco, 2023.

SACRAMENTO, Daniel. **Árvores de decisão**: entenda esse algoritmo de Machine Learning.[s.l], [2024?] . Disponível em: <https://blog.somostera.com/data-science/arvores-de-decisão>. Acesso em: 08 set. 2024.

SAIBA mais sobre seu relatório de crédito e como obter uma cópia. USA GOV, [S.l], 11 jun. 2024. Disponível em: <https://www.usa.gov/credit-reports>. Acesso em: 14 out 2024.

SARMENTO, Daniel. **Direitos Fundamentais e Relações Privadas**. Rio de Janeiro: Lumen Juris, 2008.

SCHERER, Matthew U. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. **Harvard Journal of Law & Technology**, v. 29, n. 2, 2016. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>. Acesso em: 17 set. 2024.

SEERAPIÃO. Adriane Beatriz de Souza. **Fundamentos de otimização por inteligência de enxames: uma visão geral.** Disponível em**: <**https://doi.org/10.1590/S0103-17592009000300002>. Acesso em: 08 set 2024.

SICHMAN, J. S.. Inteligência Artificial e sociedade: avanços e riscos. **Estudos Avançados**, v. 35, n. 101, p. 37–50, jan. 2021.. Disponível em: <https://www.scielo.br/j/ea/a/c4sqqrthGMS3ngdBhGWtKhh/?lang=pt>. Acesso em: 08 set 2024.

SCHOLZ, Lauren H. Algorithmic contracts. **Stanford Technology Law Review**, v. 20, n. 2, p. 128-168, set./dez. 2017.

SCHWAB, Klaus. **A quarta revolução industrial**. Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SEBE, Nakashima. Human-centered computing. In: NAKASHIMA, Hideyuki; AGHAJAN, Hamid; AUGUSTO, Juan Carlos (Orgs.). **Handbook of ambient intelligence and smart environments**. Dordrecht: Springer, p. 349-370, 2010.

SELBST, Andrew D.; BAROCAS, Solon. Intuitive Appeal of Explainable Machines. **Fordham Law Review**, v. 87, p. 1085, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3126971>. Acesso em: 07 set. 2024.

SELBST, Andrew D.; POWLES, Julia. Meaningful Information and the Right to Explanation. **International Data Privacy Law**, vol. 7(4), 233-242, 2017. Disponível em: <https://academic.oup.com/idpl/article/7/4/233/4762325> Acessado em 09 set. 2024

SERGIPE suspende uso de reconhecimento facial após abordagem errada da PM. UOL, São Paulo, 16 abr. 2024. Disponível em: <https://noticias.uol.com.br/cotidiano/ultimas-noticias/2024/04/16/sergipe-suspende-uso-de-reconhecimento-facial-apos-abordagem-errada-da-pm.htm>. Acesso em: 01 mai 2024.

SHAP. **GitHub**: slundberg/shap. Disponível em: <https://github.com/slundberg/shap>. Acesso em: 27 out 2024.

SIMÃO FILHO, Adalberto. Dano ao consumidor por invasão do site ou da rede. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (coord.). **Direito & Internet**: aspectos jurídicos relevantes. São Paulo: Edipro, 2001.

SOUSA, Priscila. Ciberespaço - O que é, estrutura, conceito e definição. **Conceito.de**, [S.l], 2023. Disponível em: <https://conceito.de/ciberespaco#:~:text=Ciberespa%C3%A7o%20remete%20ao%20espa%C3%A7o%20das,resumo%20com%20os%20pontos%2Dchave>. Acesso em: 11 de fev de 2025.

SOUZA, Renato Rocha. Sobre a ética humana e a ética dos algoritmos. In: MAGRANI, Eduardo (org.). **Horizonte presente**: debates de tecnologia e sociedade. Rio de Janeiro: Letramento, 2019.

STANCIOLI, Ana Elisa. **Incentivos e risco moral nos planos de saúde no Brasil**. 2002. Dissertação (Mestrado em Economia) – Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, São Paulo, 2002.

STAPLES, William G. **Encyclopedia of privacy**. Westport: Greenwood Press, 2007.

STF E PROTEÇÃO de dados pessoais: decisões da Corte marcaram a evolução de um novo direito fundamental. Supremo Tribunal Federal, Brasília, 14 ago. 2024. Disponível em; <https://noticias.stf.jus.br/postsnoticias/stf-e-protecao-de-dados-pessoais-decisoes-da-corte-marcaram-a-evolucao-de-um-novo-direito-fundamental/>. Acesso em: 03 fev. 2025.

STREET View. **Google,** [S.l], [20--]. Disponível em: <https://www.google.com/intl/pt-BR/streetview/>. Acesso em: 14 set. 2024.

SURDEN, Harry. Artificial Intelligence and Law: An Overview. **Georgia State University Law Review**, v. 35, n. 4, p. 1306-1337, 2019. Disponível em: <https://readingroom.law.gsu.edu/gsulr/vol35/iss4/8/>. Acesso em: 17 set. 2024.

SURDEN, Harry. Machine Learning and Law. **Washington Law Review**, v. 89, p. 87-115, 2014. Disponível em: <https://scholar.law.colorado.edu/faculty-articles/81/>. Acesso em: 08 set. 2024.

TRAURING REVISION. **Eliot:** Logging that tells you why it happened. Disponível em: <https://eliot.readthedocs.io/en/latest/>. Acesso em 31 out 2024.

TONETTO, L. M. et al.. O papel das heurísticas no julgamento e na tomada de decisão sob incerteza. **Estudos de Psicologia** (Campinas), v. 23, n. 2, p. 181–189, abr. 2006. Disponível em: <https://doi.org/10.1590/S0103-166X2006000200008>. Acesso em: 09 set. 2024.

TURING, A. M. **Computing Machinery and Intelligence**. Mind, 1950.

TYLER VIGEN. **Spurious Correlations**. Disponível em: <https://www.tylervigen.com/spurious-correlations>. Acesso em: 09 set. 2024.

UFPR. Aprendizado de Máquina. Disponível em: <https://www.inf.ufpr.br/aurora/tutoriais/aprendizadomaq/>. Acesso em: 08 set. 2024.

UNIÃO EUROPEIA. Comunicação da Comissão ao Parlamento Europeu e ao Conselho. **EUR-Lex**, 2018. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0043>. Acesso em: 10 fev. 2019.

UNIÃO EUROPEIA. Proteção de dados pessoais. **EUR-Lex**, 2024. Disponível em: <https://eur-lex.europa.eu/PT/legal-content/summary/protection-of-personal-data.html>. Acesso em: 30 mai 2024.

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados, Artigo 22. [S.l], 2024. Disponível em: <https://www.privacy-regulation.eu/pt/22.htm>. Acesso em: 27 out 2024.

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados, Considerando 99. [S.l], 2024. Disponível em: <https://gdpr-text.com/pt/read/recital-99/>. Acesso em: 26 set. 2024.

UNIÃO EUROPEIA. Regulamento Geral sobre a Proteção de Dados. **EUR-Lex**, 2018. Disponível em: <https://eur-lex.europa.eu/content/news/general-data-protection-regulation-GDPR-applies-from-25-May-2018.html?locale=pt>. Acesso em: 20 out 2024.

VALENTIM, Styvenson. **Projeto de Lei nº4496 de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), para definir a expressão "decisão automatizada". Brasília: Senado Federal, 14 ago. 2019. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/138136>. Acesso em: 27 ago. 2024.

VERASZTO, Estéfano Vizconde; SILVA, Dirceu da; MIRANDA, Nonato Assis de; SIMON, Fernanda Oliveira. **Tecnologia:** buscando uma definição do conceito. Prisma.com, n. 7, 2008.

VU, Brandon. A technological ant ethical analysis of facial recognition in tje modern era. In: **A Technological and Ethical Analysis of Facial Recognition in the Modern Era**, 2018. Disponível em: <https://www.academia.edu/38066258/A_Technological_and_Ethical_Analysis_of_Facial_Recognition_in_the_Modern_Era>. Acesso em: 05 de jun 2024.

XAVIER, Elis Cristina Nogueira; VIEGAS, Claudia, Mara de Almeida Rabelo; POLI, Leonardo Macedo. Translúcio: a explicabilidade como alternativa para a opacidade da inteligência artificial. **Revista Magister de Direito Civil e Processo Civil,** Editora Magister: Porto Alegre, v. 1, p. 8 – 27.

ZANATTA, Rafael Augusto Ferreira. Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. [S.l], fev. 2019. Disponível em: <https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais>. Acesso em: 01 out. 2024.

ZANATTA, Rafael Augusto Ferreira. Tutela coletiva e coletivização da proteção de dados pessoais. In: PALHARES, Felipe (org.). **Temas Atuais de Proteção de Dados Pessoais**. São Paulo: Revista dos Tribunais, 2020. p. 345-374.

ZARREHPARVAR, Mandana. A nondiscriminatory information society. In: JØRGENSEN, Rikke Frank (ed.). Human rights in the global information society. **Cambridge:** MIT Press, 2006.

ZARSKY, Tal. Transparent Predictions. **University of Illinois Law Review**, v. 2013, n. 4, 2013. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2324240>. Acesso em: 17 set. 2024.

ZHANG, Yongfeng; CHEN, Xu. Explainable Recommendation: A Survey and New Perpectives. **Foundations and Trends in Information Retrieval**, v. 14, n. 1, p. 1-101, 2020. Disponível em: <https://arxiv.org/abs/1804.11192>. Acesso em: 24 abr. 2024.

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

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda (org.). **Tecnopolíticas da vigilância**: perspectivas da margem. Tradução: Antonio Holzmeister Oswaldo Cruz e Bruno Cardoso. São Paulo: Boitempo, 2018.

WACHTER, Sandra; MITTELSTADT, Brent. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI. **Columbia Business Law Review**, v. 2019, n. 2, 2019. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829>. Acesso em: 04 jun. 2024.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. **International Data Privacy Law**, v. 7, n. 2, p. 76-99, maio 2017. Disponível em: <https://ssrn.com/abstract=2903469>. Acesso em: 17 fev. 2024.

WEBER, Rosa. **Pronunciamento nº 9416294.** Brasília: Supremo Tribunal Federal, 06 maio 2021. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/verPronunciamento.asp?pronunciamento=9416294>. Acesso em: 10 abril 2024.

WECHSLER, Harry. **Reliable face recognition methods:** system design, implementation and evolution. New York: Springer, 2007.

WEST, Sarah Myers; WHITTAKER, Meridith; CRAWFORD, Kate. Discriminating Systems: Gender, Race and Power in AI. **AI Now Institute**, 2019. Disponível em: <https://ainowinstitute.org/publication/discriminating-systems-gender-race-and-power-in-ai-2>. Acesso em: 14 ago. 2024.

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

WORLD ECONOMIC FORUM. Global Gender Gap Report 2021. [S.l], 30 mar. 2021. Disponível em: <https://www.weforum.org/publications/global-gender-gap-report-2021/>. Acesso em: 18 abr. 2024.

WYSE, Terezinha de Souza; HAYNE, Luiz Augusto. Análise da evolução da tecnologia: uma contribuição para o ensino da ciência e tecnologia. **Revista Brasileira de Ensino de Ciência e Tecnologia**, v. 11, n. 3, p. 37-64. DOI: 10.3895/rbect.v11n3.5947. Acesso em: 14 jun. 2024.