

**VI CONGRESSO INTERNACIONAL DE
DIREITO E INTELIGÊNCIA
ARTIFICIAL (VI CIDIA)**

**PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E
NEGÓCIOS INOVADORES II**

P961

Privacidade, proteção de dados pessoais e negócios inovadores II [Recurso eletrônico on-line]
organização VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA):
Skema Business School – Belo Horizonte;

Coordenadores: Alexandre Schmitt da Silva Mello, Mariana de Moraes Palmeira e Pietra
Daneluzzi Quinelato – Belo Horizonte: Skema Business School, 2025.

Inclui bibliografia

ISBN: 978-65-5274-361-9

Modo de acesso: www.conpedi.org.br em publicações

Tema: Perspectivas globais para a regulação da inteligência artificial.

1. GDPR. 2. Segurança da informação. 3. Compliance. I. VI Congresso Internacional de
Direito e Inteligência Artificial (1:2025 : Belo Horizonte, MG).

CDU: 34

skema
BUSINESS SCHOOL

LAW SCHOOL
FOR BUSINESS

**VI CONGRESSO INTERNACIONAL DE DIREITO E
INTELIGÊNCIA ARTIFICIAL (VI CIDIA)**
**PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E NEGÓCIOS
INOVADORES II**

Apresentação

A SKEMA Business School é uma organização francesa sem fins lucrativos, com presença em sete países diferentes ao redor do mundo (França, EUA, China, Brasil, Emirados Árabes Unidos, África do Sul e Canadá) e detentora de três prestigiadas creditações internacionais (AMBA, EQUIS e AACSB), refletindo seu compromisso com a pesquisa de alta qualidade na economia do conhecimento. A SKEMA reconhece que, em um mundo cada vez mais digital, é essencial adotar uma abordagem transdisciplinar.

Cumprindo esse propósito, o VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA), realizado nos dias 18 e 19 de setembro de 2025, em formato híbrido, manteve-se como o principal evento acadêmico sediado no Brasil com o propósito de fomentar ricas discussões sobre as diversas interseções entre o direito e a inteligência artificial. O evento, que teve como tema central a "Regulação da Inteligência Artificial", contou com a presença de renomados especialistas nacionais e internacionais, que abordaram temas de relevância crescente no cenário jurídico contemporâneo.

Profissionais e estudantes dos cursos de Direito, Administração, Economia, Ciência de Dados, Ciência da Computação, entre outros, tiveram a oportunidade de se conectar e compartilhar conhecimentos, promovendo um ambiente de rica troca intelectual. O VI CIDIA contou com a participação de acadêmicos e profissionais provenientes de diversas regiões do Brasil e do exterior. Entre os estados brasileiros representados, estavam: Alagoas (AL), Bahia (BA), Ceará (CE), Goiás (GO), Maranhão (MA), Mato Grosso do Sul (MS), Minas Gerais

Foram discutidos assuntos variados, desde a própria regulação da inteligência artificial, eixo central do evento, até as novas perspectivas de negócios e inovação, destacando como os algoritmos estão remodelando setores tradicionais e impulsionando a criação de empresas inovadoras. Com uma programação abrangente, o congresso proporcionou um espaço vital para discutir os desafios e oportunidades que emergem com o desenvolvimento algorítmico, reforçando a importância de uma abordagem jurídica e ética robusta nesse contexto em constante evolução.

A programação teve início às 13h, com o check-in dos participantes e o aquecimento do público presente. Às 13h30, a abertura oficial foi conduzida pela Prof.^a Dr.^a Geneviève Poulingue, que, em sua fala de boas-vindas, destacou a relevância do congresso para a agenda global de inovação e o papel da SKEMA Brasil como ponte entre a academia e o setor produtivo.

Em seguida, às 14h, ocorreu um dos momentos mais aguardados: a Keynote Lecture do Prof. Dr. Ryan Calo, renomado especialista internacional em direito e tecnologia e professor da University of Washington. Em uma conferência instigante, o professor explorou os desafios metodológicos da regulação da inteligência artificial, trazendo exemplos de sua atuação junto ao Senado dos Estados Unidos e ao Bundestag alemão.

A palestra foi seguida por uma sessão de comentários e análise crítica conduzida pelo Prof. Dr. José Luiz de Moura Faleiros Júnior, que contextualizou as reflexões de Calo para a realidade brasileira e fomentou o debate com o público. O primeiro dia foi encerrado às 14h50 com as considerações finais, deixando os participantes inspirados para as discussões do dia seguinte.

As atividades do segundo dia tiveram início cedo, com o check-in às 7h30. Às 8h20, a Prof.^a Dr.^a Margherita Pagani abriu a programação matinal com a conferência Unlocking Business Creativity Using Artificial Intelligence, apresentando insights sobre como a IA pode

Após um breve e merecido coffee break às 9h40, os participantes retornaram para uma manhã de intensas reflexões. Às 10h30, o pesquisador Prof. Dr. Steve Ataky apresentou a conferência Regulatory Perspectives on AI, compartilhando avanços e desafios no campo da regulação técnica e ética da inteligência artificial a partir de uma perspectiva global.

Encerrando o ciclo de palestras, às 11h10, o Prof. Dr. Filipe Medon trouxe ao público uma análise profunda sobre o cenário brasileiro, com a palestra AI Regulation in Brazil. Sua exposição percorreu desde a criação do Marco Legal da Inteligência Artificial até os desafios atuais para sua implementação, envolvendo aspectos legislativos, econômicos e sociais.

Nas tardes dos dois dias, foram realizados grupos de trabalho que contaram com a apresentação de cerca de 60 trabalhos acadêmicos relacionados à temática do evento. Com isso, o evento foi encerrado, após intensas discussões e troca de ideias que estabeleceram um panorama abrangente das tendências e desafios da inteligência artificial em nível global.

Os GTs tiveram os seguintes eixos de discussão, sob coordenação de renomados especialistas nos respectivos campos de pesquisa:

a) Startups e Empreendedorismo de Base Tecnológica – Coordenado por Allan Fuezi de Moura Barbosa, Laurence Duarte Araújo Pereira, Cildo Giolo Júnior, Maria Cláudia Viana Hissa Dias do Vale Gangana e Yago Oliveira

b) Jurimetria Cibernética Jurídica e Ciência de Dados – Coordenado por Arthur Salles de Paula Moreira, Gabriel Ribeiro de Lima, Isabela Campos Vidigal Martins, João Victor Doreto e Tales Calaza

c) Decisões Automatizadas e Gestão Empresarial / Algoritmos, Modelos de Linguagem e Propriedade Intelectual – Coordenado por Alisson Jose Maia Melo, Guilherme Mucelin e

f) Regulação da Inteligência Artificial – III – Coordenado por Ana Júlia Silva Alves Guimarães, Erick Hitoshi Guimarães Makiya, Jessica Fernandes Rocha, João Alexandre Silva Alves Guimarães e Luiz Felipe Vieira de Siqueira

g) Inteligência Artificial, Mercados Globais e Contratos – Coordenado por Gustavo da Silva Melo, Rodrigo Gugliara e Vitor Ottoboni Pavan

h) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – I – Coordenado por Dineia Anziliero Dal Pizzol, Evaldo Osorio Hackmann, Gabriel Fraga Hamester, Guilherme Mucelin e Guilherme Spillari Costa

i) Privacidade, Proteção de Dados Pessoais e Negócios Inovadores – II – Coordenado por Alexandre Schmitt da Silva Mello, Lorenzo Antonini Itabaiana, Marcelo Fonseca Santos, Mariana de Moraes Palmeira e Pietra Daneluzzi Quinelato

j) Empresa, Tecnologia e Sustentabilidade – Coordenado por Marcia Andrea Bühring, Ana Cláudia Redecker, Jessica Mello Tahim e Maraluce Maria Custódio.

Cada GT proporcionou um espaço de diálogo e troca de experiências entre pesquisadores e profissionais, contribuindo para o avanço das discussões sobre a aplicação da inteligência artificial no direito e em outros campos relacionados.

Um sucesso desse porte não seria possível sem o apoio institucional do Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, que desde a primeira edição do evento provê uma parceria sólida e indispensável ao seu sucesso. A colaboração contínua do CONPEDI tem sido fundamental para a organização e realização deste congresso, assegurando a qualidade e a relevância dos debates promovidos.

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Ms. Dorival Guimarães Pereira Júnior

Coordenador do Curso de Direito – SKEMA Law School

Prof. Dr. José Luiz de Moura Faleiros Júnior

Coordenador de Pesquisa – SKEMA Law School

ERA DIGITAL PRIVACIDADE E PROTEÇÃO DE DADOS UMA ANÁLISE ECONÔMICA E JURÍDICA

PRIVACY AND DATA PROTECTION IN THE DIGITAL ERA: AN ECONOMIC AND LEGAL ANALYSIS

Luiz Felipe Vieira de Siqueira ¹
Rita de Cassia de Oliveira Sebastiao

Resumo

Este artigo, intitulado "Era Digital Privacidade e Proteção de Dados uma Análise Econômica e Jurídica", examina os desafios e oportunidades da privacidade e proteção de dados na era digital, com foco na formação do mercado global e brasileiro. A pesquisa baseou-se em revisão bibliográfica e análise teórica das legislações e implicações econômico-sociais. Constatou-se que a ubiquidade de dados pessoais e escândalos como Snowden e Cambridge Analytica impulsionaram a criação de normativas como GDPR e LGPD. Essas leis fomentaram um mercado emergente de serviços e tecnologias em cibersegurança, consultoria jurídica e gestão de dados, além da profissão de Encarregado de Dados (DPO). No Brasil, apesar dos avanços regulatórios da LGPD e da ANPD, persistem desafios relacionados à desinformação, baixa conformidade empresarial e fiscalização, como ilustrado pelo caso Meta. Conclui-se que o fortalecimento desse mercado é essencial para equilibrar inovação tecnológica e direitos fundamentais.

Palavras-chave: Privacidade de dados, Proteção de dados, Lgpd, Inteligência artificial, Mercado digital

Abstract/Resumen/Résumé

This article, titled "Digital Era Privacy and Data Protection: An Economic and Legal Analysis," examines the challenges and opportunities of privacy and data protection in the digital age, with a focus on the formation of the global and Brazilian markets. The research was based on a literature review and theoretical analysis of legislation and socio-economic implications. It was found that the ubiquity of personal data and scandals such as Snowden

Keywords/Palabras-claves/Mots-clés: Data privacy, Data protection, Lgpd, Artificial intelligence, Digital market

1. INTRODUÇÃO

A evolução humana foi pautada na capacidade do homem de se comunicar, locomover, educar a prole, cultivar e obter os próprios alimentos.

A Revolução Industrial no século XIX transformou o mundo da agricultura, pecuária e manufatura na produção em larga escala o que gerou, consequentemente, o consumo de massa.

Dessa forma, os riscos que envolvem a produção em escala industrial são muito maiores do que na manufatura, tanto na confecção pelos trabalhadores quanto para os consumidores, dado a proporção que este alcançou. A contaminação de uma simples bactéria no processamento de um produto alimentício pode ocasionar em sérios danos à saúde e até em óbitos. Ao mesmo tempo, um curto-circuito em uma fábrica pode ocasionar uma explosão, incêndio e levar a morte dos trabalhadores.

A evolução tecnológica e o advento da sociedade pós-industrial na segunda metade do século XX potencializou os riscos, pois a escala com que os produtos e as formas de preparo foram extremamente ampliados. Um forte exemplo disso é o acidente com a Usina Nuclear de Chernobyl na Ucrânia em 1986, o qual matou milhares de pessoas de forma direta e outros milhares de forma indireta através do câncer gerado em consequência do desastre.

Com o advento da Internet no final dos anos 60 e, principalmente com o seu uso comercial a partir dos anos 90 com a *world wide web*, deu-se origem a maior revolução tecnológica da humanidade – a era digital. A ditadura geográfica foi quebrada, as barreiras tecnológicas se romperam, as fronteiras do mundo, de uma certa forma, ruíram e, consequentemente, a falta de conhecimento se transformou em excesso de informação. Paradoxalmente, o excesso de informação acarreta a desinformação, um grande mal da era digital.

Até o final do século XX, para se obter conhecimento de outras culturas ou de assuntos específicos o homem tinha que se locomover por grandes distâncias, pesquisar inúmeras bibliotecas, obter milhares de fotocópias, para, então, ter em mãos o conteúdo para o seu trabalho ou pesquisa.

Da mesma forma, a troca de correspondências era feita através de telex, cartas e telefonemas e, dado o alto custo e à baixa tecnologia, essa tarefa se estendia por muito tempo.

Hoje em dia, a humanidade se comunica em tempo real, a baixo custo de transação, seja qual for a distância entre os interlocutores. O conhecimento vem sendo digitalizado e disponibilizado em grande escala na Internet, formando, assim, a sociedade da informação.

A informação e o conhecimento, que antes eram um problema, hoje já não são mais. O grande desafio, agora, é filtrar a informação e obter aquela mais adequada para o estudo, pesquisa ou trabalho.

E essa é a IV Revolução Industrial que iniciou no fim do século XX com a chegada da Internet. Agora, em tempos de Inteligência Artificial existe um debate se estamos adentrando em uma nova revolução industrial ou se está iniciando um novo tipo de transformação.

Hoje, os humanos podem trabalhar de casa, comprar produtos e adquirir serviços de todas as naturezas por vias digitais e em diferentes partes do Planeta Terra.

Entretanto, a humanidade desde o início da Internet vem deixando as suas pegadas e, principalmente, os seus dados pessoais no ambiente virtual. As pessoas registram os seus dados pessoais em qualquer plataforma, tais como: nome, telefone, CPF, endereço, número do cartão de crédito, localização geográfica, fotos, *nudes*, renunciando aos princípios constitucionais e fundamentais da privacidade e da proteção de dados.

Existe um tratamento em larga escala de dados pessoais no Ciberespaço o que gerou escândalos como os casos Snowden¹ que deu o título de filme e motivou o Marco Civil da Internet, bem como do escândalo *Cambridge Analytica* muito bem retratado no documentário *The Great Hack*² que retrata, dentre outras coisas intrigantes, uma das razões que ensejaram a edição da Lei Geral de Proteção de Dados no Brasil. Vale destacar que a *Cambridge Analytica* desempenhou um papel crucial em dez eleições ao longo de sua existência, sem registrar derrotas. Entre os exemplos mais notáveis estão as eleições presidenciais em Trinidad e Tobago, o referendo do *Brexit* e a primeira campanha presidencial de Donald Trump de 2016.

A União Europeia possui um histórico de proteção de dados. Vale lembrar que a primeira máquina de inteligência artificial que se tem notícia no mundo foi criada

¹ <https://www.primevideo.com/-/pt/detail/Snowden/0NHF2PS2PDAZUNPQUPB5SCL3R6> , acesso em 13 de março de 2025.

² <https://www.netflix.com/title/80117542> , acesso em 13 de março de 2025.

pelo matemático inglês Alan Turin para decodificar as mensagens codificadas enviadas pelos alemães por via da máquina Enigma. Há quem diga que diante da captura e decodificação das mensagens dos nazistas que a II Guerra Mundial teve o seu fim abreviado. Uma parte da grande história de Turin está retratada na obra cinematográfica “O Jogo da Imitação”. O matemático britânico também deu nome ao Prêmio Turing que é tido como o “Prêmio Nobel da Computação” e é concedido desde 1966.

A União Europeia debateu sobre privacidade e proteção de dados por quatro anos. Em 25 de maio de 2016 o *General Data Protection Regulation* (GDPR) foi promulgada, sendo que a norma entrou em vigor após dois anos de *vacatio legis*. A legislação europeia é bastante restritiva para as Organizações e protetiva quanto aos titulares dos dados pessoais. A norma é obrigatória para empresas com mais de duzentos e cinquenta funcionários, art. 30 GDPR.

A República Popular da China possui um arcabouço jurídico robusto em termos de proteção de dados, com destaque para a Lei de Proteção de Informações Pessoais (Personal Information Protection Law - PIPL). Esta legislação estabelece parâmetros rigorosos para a coleta, armazenamento e uso de dados pessoais, mas também levanta preocupações em termos de supervisão governamental e liberdades individuais.

O artigo 3º do PIPL introduz um conceito curioso: os "dados pessoais estratégicos". Esse termo remete a informações de importância crítica, que, sob a lei, são armazenadas em servidores interconectados diretamente ao governo. Este modelo permite uma ampla supervisão estatal, atribuindo ao governo chinês um nível de controle enorme sobre dados estratégicos, incluindo aqueles de natureza pessoal.

Antes mesmo da implementação do PIPL em 2021, a China já possuía legislações voltadas à privacidade e proteção de dados, como as Leis de Cibersegurança e de Segurança Nacional, promulgadas até janeiro de 2018. No entanto, o PIPL consolidou muitas das diretrizes anteriores, articulando uma visão integrada de governança de dados.

Nos Estados Unidos, a abordagem à proteção de dados é fragmentada e marcada pela ausência de uma legislação federal abrangente, reflexo do forte federalismo do país. As normas que regulam dados pessoais são dispersas e variam de estado para estado. Entre elas, destaca-se a lei da Califórnia, conhecida como CCPA (*California Consumer Privacy Act*), que apresenta padrões mais restritivos e é frequentemente comparada ao Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. Ainda assim, essa

lei estadual, embora significativa, não substitui a necessidade de uma estrutura nacional unificada.

Em 1995, a União Europeia determinou que os Estados Unidos não dispunham de um nível adequado de proteção para dados pessoais, o que trouxe desafios às transferências de informações entre essas regiões. Para contornar essa incompatibilidade, foi estabelecido o acordo Safe Harbor em 2000, que funcionava como uma garantia de que empresas americanas que aderiam às suas regras respeitariam padrões mínimos de proteção. No entanto, esse acordo foi anulado pela Corte de Justiça Europeia em 2015 em virtude de uma ação judicial promovida pelo ativista Max Schrems, após preocupações relacionadas à segurança dos dados e à supervisão insuficiente.

Como resposta, surgiu o Privacy Shield em 2016, uma tentativa de oferecer maior proteção e transparência nas transferências de dados entre a União Europeia e os Estados Unidos. A natureza jurídica do Privacy Shield é controversa e geralmente caracterizada como um tratado comercial entre EUA e EU. Apesar das melhorias prometidas, o Privacy Shield também enfrentou críticas também lideradas por Schrems e acabou sendo invalidado pela Corte de Justiça Europeia em 2020. Desde então, houve esforços para criar um novo acordo.

Em 2022, líderes dos EUA e da UE anunciaram um novo framework chamado *Trans-Atlantic Data Privacy Framework*, que busca substituir o Privacy Shield. Esse novo acordo foi formalizado em julho de 2023, quando a Comissão Europeia adotou uma decisão de adequação para o *EU-US Data Privacy Framework*. Ele introduz salvaguardas vinculativas para limitar o acesso aos dados por agências de inteligência dos EUA e estabelece um mecanismo independente de resolução de disputas para cidadãos europeus.

A América Latina apresenta abordagens diversificadas em relação à proteção de dados, especialmente no caso do Uruguai e da Argentina, dois países que se destacam neste cenário, sendo ambos reconhecidos como tendo níveis adequados sobre a matéria pela União Europeia. Enquanto isso, outros países promulgaram normas sobre privacidade e proteção de dados como o Chile (1999), Paraguai (2001), México (2010) e Peru (2011).

Já o Brasil, não tinha qualquer norma de proteção de dados em vigor até o segundo semestre de 2018.

A Lei Geral de Proteção de Dados no Brasil foi aprovada com a implantação de uma Autoridade de Proteção de Dados, que seria uma Autoridade Supervisora independente, como o exemplo europeu. A LGPD foi sancionada em 14 de agosto de

2018, entrou em vigor em setembro de 2020 e suas sanções podem ser aplicadas desde agosto de 2021.

A Medida Provisória 869/2018 trouxe mudanças significativas na estrutura da Autoridade Nacional de Proteção de Dados (ANPD). Posteriormente, essa medida foi convertida na Lei 13.853/19, vinculando a ANPD à Casa Civil da Presidência da República e estipulando uma revisão estrutural após dois anos de sua eficácia. Em 26 de outubro de 2022, a Lei 14.460/22 foi sancionada, transformando a ANPD em uma autarquia federal ligada ao Ministério da Justiça. Apesar das mudanças, o debate sobre a verdadeira independência da Autoridade permanece.

Em 10 de fevereiro de 2022 entrou em vigor a Emenda Constitucional 115 e instituiu o inciso LXXIX no artigo 5º da Constituição da República, garantindo a proteção de dados como um direito fundamental no Brasil.

Tal qual a GDPR a LGPD é bastante restritiva para as Organizações e muito protetiva aos titulares dos dados. O cumprimento LGPD é obrigatório para empresas e entes públicos sem distinção de tamanho ou número de funcionários.

Registre-se que o Brasil é uma nação de baixa escolaridade e com voto obrigatório por Lei. A desinformação aliada a proliferação de *Fake News* e a imaturidade quanto aos direitos da privacidade e proteção de dados, faz do Brasil um alvo fácil para o fomento de organizações que querem levar vantagem financeira, comercial e eleitoral de ignorantes para vender produtos (muitas vezes desnecessários) e eleger candidatos com forte poder econômico e atuação nas redes sociais.

As normas de privacidade e proteção de dados proliferam no mundo para garantir o equilíbrio entre a inovação e os direitos fundamentais. Um novo mercado foi formado com essa dualidade e é isso que será tratado neste artigo.

2. METODOLOGIA

A metodologia adotada neste artigo ancora-se predominantemente na revisão bibliográfica e na análise teórica aprofundada. Inicialmente, explora-se o arcabouço conceitual de teorias econômicas clássicas e contemporâneas.

O artigo desenvolve também um enfoque crítico sobre a legislação de proteção de dados no mundo, analisando e ponderando suas implicações econômicas e sociais. A análise engloba a discussão sobre a formação e as dinâmicas do mercado de privacidade,

o papel central das grandes empresas tecnológicas nesse cenário, o impacto regulatório e a atuação das Autoridades Supervisoras.

3. BIG TECHS E ECONOMIA NA ERA DIGITAL: DESAFIOS E POSSIBILIDADES

3.1. Contextualizando a sociedade Pós-Industrial

A sociedade pós-industrial, marcada por eventos como o desembarque na Normandia (1944), a descoberta do DNA (1953) e a crise petrolífera (1973), reflete transformações significativas na economia e na organização social.

Os aspectos determinantes desta sociedade incluem a transição da produção de bens para serviços, a valorização da classe profissional e técnica, e o saber teórico como fonte de inovação. Além disso, a gestão do desenvolvimento técnico e o controle da tecnologia tornam-se centrais, juntamente com a criação de uma nova tecnologia intelectual (DE MASI, 2003, p. 35). Empresas de comunicação e tecnologia, ao realizarem grandes operações financeiras, consolidam sua influência, promovendo a assimetria da informação e ditando tendências de mercado. Como destaca Bagnoli, "a grande empresa impõe valores e promove a assimetria da informação, fazendo o consumidor adquirir aquilo que ela queira produzir e vender" (BAGNOLI, 2009, p. 59).

A transição da sociedade industrial para a pós-industrial decorre da evolução tecnológica e da migração da mão-de-obra para o setor de serviços, representando a passagem dos átomos para os bits e da era da informação para a pós-informação.

O narcisismo, reforçado pela massificação do consumo, emerge como traço característico da personalidade dos indivíduos na era digital com a proliferação das redes sociais (DE MASI, 2003). Indústrias de comunicação e Big Techs moldam os consumidores, vulneráveis ao aparato tecnológico os mantém viciados em suas redes. Estas empresas, determinantes do poder econômico, criam produtos que, na era digital, intensificam riscos à sociedade e, até a sobrevivência no planeta. O avanço da ciência versus o risco e os danos que ela pode causar é o conflito essencial da era digital, afetando empresas, mercados e a economia global.

As Big Techs, representadas por conglomerados globais como Google, Amazon, Meta, Apple e Microsoft, desempenham um papel central na dinâmica da sociedade pós-industrial e na economia digital. Essas empresas dominam não apenas o

mercado de tecnologia, mas também áreas-chave como comunicação, comércio eletrônico e, sobretudo, o tratamento de dados, inclusive, pessoais.

A convergência entre tecnologia, telecomunicações e finanças transforma as Big Techs em verdadeiros atores globais, capazes de moldar padrões de comportamento, ditar tendências de consumo e influenciar decisões políticas. Como argumenta Bagnoli (2009, p. 59), "não é o mercado que dita as regras, mas a grande empresa", que, por meio de seu poder econômico, promove assimetrias de informação e direciona a sociedade para adquirir o que ela própria define como necessário.

Apesar disso, as Big Techs também são responsáveis por avanços tecnológicos fundamentais, como a inteligência artificial e ferramentas de otimização de processos que beneficiam diversas indústrias e áreas do conhecimento.

3.2. O papel dos Dados e da Informação na Economia

A informação desempenha um papel fundamental na economia, especialmente no dinâmico mercado de tecnologia. Ela possui características únicas que a distinguem dos bens tradicionais e impulsionam o desenvolvimento e a inovação (JONES, 2020).

Em primeiro lugar, a informação pode ser vista como um bem econômico valioso e custoso de se obter. No setor de tecnologia, a aquisição e o uso de informação técnica, ou seja, o conhecimento necessário para produzir bens, são essenciais para as empresas. A própria organização da indústria e o comportamento competitivo das firmas estão intrinsecamente ligados ao papel da informação na produção (ARROW, 1996).

Ademais, a informação, particularmente na forma de dados, possui a característica de ser não-rival. Isso significa que ela pode ser utilizada simultaneamente por inúmeras empresas e indivíduos sem se esgotar ou diminuir sua disponibilidade para outros. Exemplos como grandes conjuntos de imagens rotuladas ou dados de localização podem ser usados repetidamente em processos produtivos, incluindo a criação de novas ideias. Nesse sentido, os dados são um fator de produção crucial na economia moderna, impulsionando avanços em áreas como carros autônomos, tradução em tempo real e inteligência artificial (JONES, 2020).

A gestão da informação é, portanto, um processo crítico para as organizações, envolvendo o planejamento, coleta, organização, utilização, controle, disseminação e descarte eficiente de suas informações para identificar e explorar seu valor máximo.

Contudo, a informação também apresenta desafios únicos. Sua definição e mensuração em termos gerais podem ser complexas. Além disso, a assimetria de informação entre agentes econômicos tem implicações estratégicas importantes, influenciando a formação de instituições e as interações econômicas (Williamson, 1985).

A Internet revolucionou a forma como a informação é criada, distribuída e acessada, transformando-nos em uma "era informacional" (CASTELLS, 1999). A rede digital permite que a cultura seja capturada, criticada, comentada e distribuída instantaneamente para muitas pessoas (LESSIG, 2004).

A concentração e integração dos meios de comunicação também podem impactar a criatividade, pois grandes empresas podem ter incentivos para ignorar novas tendências culturais que não se alinham com seus negócios principais.

A informação é um pilar da economia, especialmente no setor de tecnologia. Sua natureza não-rival e sua capacidade de impulsionar a inovação a tornam um ativo estratégico crucial. No entanto, sua gestão, proteção e o equilíbrio entre propriedade intelectual e a proteção de direitos e garantias fundamentais dos seres humanos representam desafios importantes na era digital. Compreender as dinâmicas da informação é essencial para o desenvolvimento econômico e tecnológico sustentável.

3.3 O Papel do Empreendedor e a Ética na Era Digital

Schumpeter, em seu livro "Teoria Do Desenvolvimento Econômico" (1911), destaca o papel do empreendedor e da inovação no desenvolvimento econômico. Entretanto, os novos empresários não devem ter uma visão de conquistar cada vez mais usuários a nível global para os colonizar pelo vício da atenção. Esse vício é muito bem retratado no documentário “O Dilema das Redes”³.

No âmbito da produção, a informação técnica é uma característica definidora de uma empresa. Embora parte dessa informação possa estar documentada em materiais

³ <https://www.netflix.com/br/title/81254224> acesso em 14 de março de 2025.

escritos e bancos de dados, uma parcela significativa, e frequentemente a mais importante, reside no conhecimento tácito e nas habilidades dos indivíduos que compõem a empresa (ARROW, 1996). A capacidade de criar softwares e, agora Inteligência Artificial Generativa, por exemplo, está mais ligada ao conhecimento incorporado nas mentes dos programadores e dos empreendedores do que nos próprios programas existentes.

Como exemplo, tem-se o lema "Don't be evil", introduzido em 2000 por Paul Buchheit e Amit Patel, tornou-se um símbolo do compromisso ético do Google, refletindo a intenção de evitar práticas prejudiciais aos usuários e promover uma atuação justa. Parte do Código de Conduta da empresa, essa expressão passou por alterações em 2015, após a reestruturação sob a empresa-mãe Alphabet, sendo substituída por "Do the right thing". Embora tenha sido removida da introdução do código de conduta em 2018, a expressão "Don't be evil" ainda continua sendo mencionado na última linha do citado Código de Conduta⁴.

Em 2008 a Google adquiriu a DoubleClick pelo Google. A DoubleClick era uma empresa de publicidade digital que coletava dados de usuários para exibir anúncios personalizados. Com a aquisição, o Google passou a integrar esses dados com suas próprias informações de usuários, aumentando significativamente a capacidade de segmentação de anúncios.

O citado vício de atenção instituído na era digital prolifera e afeta diretamente os humanos, em especial crianças e adolescentes. A Organização das Nações Unidas (ONU) aborda os direitos das crianças em relação ao ambiente digital por meio de documentos como o Comentário Geral nº 25 de 2021⁵, emitido pelo Comitê de Direitos da Criança. Esse comentário vincula a interpretação dos direitos previstos na Convenção sobre os Direitos da Criança ao contexto digital, destacando a necessidade de proteger crianças contra riscos *online*, incluindo o uso inadequado de seus dados pessoais. Ele também enfatiza que o interesse maior da criança deve ser considerado primordialmente em todas as decisões que envolvam o ambiente digital.

A dualidade entre exposição pessoal nas redes sociais e a proteção dos dados é evidente. Normas de proteção de dados são essenciais para equilibrar o ambiente virtual,

⁴ What Google's 'Don't Be Evil' Slogan Can Teach You About Creating Your Company's Motto (forbes.com), acesso em 14 de setembro de 2024.

⁵ <https://alana.org.br/wp-content/uploads/2023/10/comentarios-gerais-portugues.pdf>. Acesso em 20 de março de 2025.

que, paradoxalmente, promove uma sensação de impunidade enquanto manipula os usuários através dos dados pessoais que eles mesmos fornecem. Além disso, empresas e governos imputam informações continuamente na rede. Na internet, o jargão “se você tem um alvo, você passa a ser o alvo” reflete a realidade de usuários bombardeados com publicidade, propagandas e mecanismos destinados à coleta e tratamento de dados pessoais em larga escala, potencializados pelo Big Data.

4. A FORMAÇÃO DO MERCADO DE PRIVACIDADE E PROTEÇÃO DE DADOS NO MUNDO E NO BRASIL

4.1. O Conceito de Mercado: Uma Análise Teórica

Max Weber define o mercado como uma forma de ação social econômica orientada pela expectativa de oportunidades de troca para obtenção de vantagens econômicas. Segundo o autor, o mercado envolve a competição entre múltiplos atores que buscam maximizar seus interesses (WEBER, 1994). A formação do mercado de privacidade pode ser entendida como uma resposta à demanda por segurança e conformidade, onde diversos fornecedores competem para oferecer as melhores soluções.

Richard Nelson e Sidney Winter, em sua perspectiva microeconômica, consideram o mercado um processo seletivo que favorece as empresas com rotinas e capacidades mais eficientes e adaptadas ao ambiente. Segundo os autores, "o mercado é um mecanismo de seleção que premia a inovação e a adaptação" (NELSON; WINTER, 1982). No contexto do mercado de privacidade, as empresas que desenvolvem tecnologias e serviços mais eficazes na proteção de dados e na conformidade com as leis tendem a prosperar.

Neil Fligstein e Jens Beckert, inspirados em Swedberg, adotam uma abordagem mais sociológica, enfatizando as estruturas sociais e culturais que moldam os mercados. Eles argumentam que "os mercados não são apenas arenas de troca, mas também são construídos por normas, regras, instituições e redes de relacionamento" (FLIGSTEIN; BECKERT, 2006). No mercado de privacidade, a confiança nas soluções oferecidas, a reputação dos fornecedores e a influência de órgãos reguladores, como a ANPD, são elementos cruciais.

Israel Kirzner propõe que o mercado é impulsionado pelo empreendedorismo e pela constante descoberta de novas oportunidades. Conforme o autor, "o empreendedor

identifica necessidades não atendidas e desenvolve soluções inovadoras que beneficiam o mercado como um todo" (KIRZNER, 1973). No mercado de privacidade, o surgimento de novas tecnologias de proteção de dados e de soluções inovadoras para a conformidade legal reflete essa dinâmica empreendedora.

4.2. O novo mercado de privacidade e proteção de dados

A crescente importância da privacidade e proteção de dados na era digital tem impulsionado a formação de um mercado global dedicado a garantir esses direitos. A promulgação de leis de proteção de dados em diversos países, como Regulamento Geral de Proteção de Dados (GDPR) na Europa e a Lei Geral de Proteção de Dados (LGPD) no Brasil, não apenas estabeleceu obrigações para organizações que tratam dados pessoais, mas também fomentou o surgimento de um mercado de serviços e tecnologias voltados à conformidade, cibersegurança e segurança da informação.

A preocupação com a privacidade acompanha a evolução tecnológica, intensificando-se com a capacidade de coleta e armazenamento de dados em larga escala pelas Organizações. O reconhecimento da privacidade e da proteção de dados como direitos fundamentais, conforme expresso na Constituição da República do Brasil, na LGPD e em legislações internacionais como a GDPR, constituiu um marco crucial para a emergência do mercado de privacidade. (CORRÊA, 2024).

A crescente importância econômica dos dados pessoais, frequentemente referidos como o "novo petróleo"⁶ na era do capitalismo de vigilância, impulsionou modelos de negócios baseados na monetização dessas informações. Empresas que coletam e monitoram dados pessoais para fins comerciais e de modulação comportamental tornaram a proteção desses dados um diferencial competitivo e uma necessidade legal (ZUBOFF, 2019).

A necessidade de conformidade com as leis de proteção de dados gerou uma demanda por serviços especializados, incluindo cibersegurança, consultorias jurídicas, implementação de medidas de segurança da informação, desenvolvimento de tecnologias de proteção de dados e a figura do Encarregado de Dados (*Data Protection Officer*), nova

⁶ Expressão cunhada pelo matemático britânico Clive Humby em 2006

profissão que é obrigatória nas organizações, tanto na GDPR (Art. 39) quanto na LGPD (art.41).

Assim, um novo mercado de cursos para formação de encarregado de dados foi inserido no planeta, bem como as certificações. As certificações mais conhecidas são EXIN (*Examination Institute for Information Science*) e a IAPP (*International Association of Privacy Professionals*). Milhares de pessoas já foram certificadas, sendo que essas empresas começaram a fornecer também cursos de LGPD em virtude da grande procura dos brasileiros para obter a formação.

4.3. Serviços e Produtos voltados para o Mercado de Privacidade e Proteção de Dados Pessoais

Os serviços e produtos voltados à privacidade e proteção de dados constituem um mercado em expansão, tanto no cenário mundial quanto no Brasil. A crescente importância da privacidade, impulsionada por legislações específicas e pela maior conscientização dos titulares de dados, fomenta a demanda por soluções que auxiliem as organizações a garantir a segurança e o tratamento adequado das informações pessoais.

No âmbito dos serviços, diversas empresas e profissionais oferecem consultoria para a adequação às leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) em nível internacional. Essa consultoria abrange a análise de processos internos, a identificação de riscos e a implementação de medidas técnicas, organizacionais e administrativas para a conformidade, com amparo na Lei e em normas técnicas, tais como *ITIL*, *NIST Cybersecurity Framework* e normas técnicas *ISO*, em especial 27000, 27001, 27002 e 27701. Segundo o Gartner os gastos globais com segurança da informação tendem a crescer 15% em 2025, estimado em US\$ 212 bilhões⁷.

Um serviço fundamental nesse contexto é o mapeamento de dados pessoais dentro das organizações, resultando em um inventário detalhado das informações coletadas, processadas e armazenadas.

A elaboração de documentos jurídicos regulatórios é outro serviço crucial, incluindo a criação de Códigos de Conduta, Políticas de Privacidade Interna e Externa,

⁷ <https://www.gartner.com/en/cybersecurity/topics/cybersecurity-program> . Acesso em 03 de abril de 2025.

que descrevem como as empresas coletam, utilizam, armazenam e compartilham dados pessoais. Há, ainda, a Política de Segurança da Informação que estabelece diretrizes para a manutenção da confidencialidade, integridade e disponibilidade dos ativos informacionais. Também se faz necessário estipular cláusulas nos contratos que exibam de forma transparente como será preservada a privacidade e a proteção dos dados pessoais dos titulares. Para transferência internacional de dados faz-se necessário distinguir se está sendo realizada para países com alto nível de maturidade na matéria. Ainda, esta transferência internacional de dados precisa ser instrumentalizada, seja pela adoção de cláusulas contratuais padrão, cláusulas específicas ou normas contratuais globais, conforme artigos 33, 34 e 35 da LGPD e Resolução 19 da ANPD. Entretanto, ainda não há indícios de que o Brasil apresente um alto grau de maturidade e carece do reconhecimento internacional para tanto.

A implementação de medidas de segurança técnicas e administrativas para proteger os dados de acessos não autorizados, perdas ou danos e o treinamento e conscientização das equipes sobre as melhores práticas de privacidade são igualmente importantes para gerar a cultura de proteção de dados. A designação e atuação de um Encarregado de Dados (DPO), obrigatória para as Organizações no Brasil, art. 41 LGPD, pessoa responsável por monitorar a conformidade com a LGPD e atuar como ponto de contato com os titulares e a Autoridade Nacional de Proteção de Dados (ANPD). A exceção à essa regra fica para *startups* e empresas do terceiro setor que não tratem dados pessoais em larga escala, conforme Resolução nº 2/2022 da Autoridade Nacional de Proteção de Dados (ANPD).

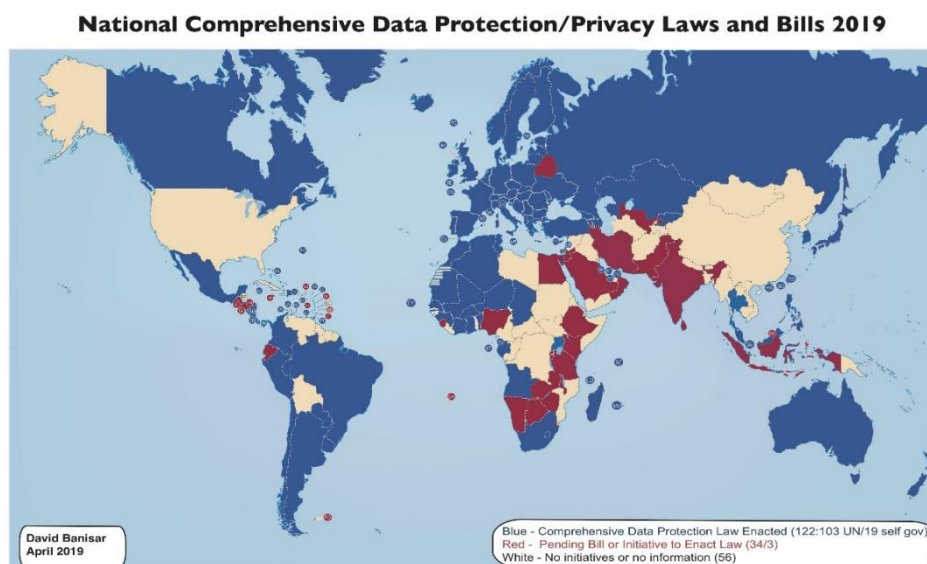
A resposta a incidentes de segurança, realização de análise de riscos, inventário de sistemas e a elaboração de Relatórios de Impacto à Proteção de Dados Pessoais (RIPD) também constituem serviços especializados. A implementação de abordagens de Privacidade por Design e por Default também são oferecidas como serviços para mitigar riscos à privacidade. O ciclo de vida dos dados, com prazos de retenção e descarte fundamentados, também consiste em um trabalho essencial para este novo mercado. Ter um ROPA (*Record of Processing Activities*) resumindo toda essa gama de processos, medidas, temporalidade dos dados é essencial e frequentemente requisitado por outras organizações em auditorias e *compliance digital*.

No que tange aos produtos, o mercado oferece plataformas de gestão de privacidade que auxiliam na automação de tarefas de conformidade, mapeamento de

dados e gestão de consentimento. Ferramentas de anonimização e pseudonimização, soluções de criptografia – como as *Privacy Enhancing Technologies* (PETs) e softwares de monitoramento e alerta de segurança são exemplos de produtos tecnológicos disponíveis. Ainda, a contratação de empresas de cibersegurança com adoção de medidas técnicas e a implementação de monitoramento da rede, IPs, firewall, antivírus, DLP, dentre outros estão entre os serviços e produtos neste mercado.

A figura 1 abaixo representa o mapa de David Banisar sobre as normas de privacidade e proteção de dados no mundo, bem como da adoção de Autoridades Supervisoras em 2018 – ano da promulgação da LGPD.

Figura 1.



Em 2018 o Brasil não tinha sequer Lei sobre Privacidade e Proteção de Dados. Até 2022, a ANPD estava ligada à Presidência da República. Em 2023, com o Decreto 11.348/23, foi vinculada ao Ministério da Justiça, alimentando o debate sobre sua independência.

A ANPD enfrenta desafios relevantes, destacando-se na promoção da cultura de privacidade e proteção de dados, mas ainda precisa avançar na fiscalização, especialmente na aplicação de sanções da LGPD. A primeira multa, de R\$ 14.400,00, foi aplicada em julho de 2023 à empresa *Telekall Infoservice*, apesar das penalidades estarem vigentes desde agosto de 2021.

No ano eleitoral de 2024, a Meta anunciou testes sua Inteligência Artificial em dados pessoais no Facebook e Instagram. O direito de oposição, obrigatório no tratamento com base no legítimo interesse, foi dificultado por estar oculto em oito etapas complexas nas plataformas.

A controvérsia teve início em 2 de julho de 2024, quando a ANPD emitiu uma medida preventiva determinando documentação que a Meta atestasse a adequação da Política de Privacidade, mediante a exclusão do trecho correspondente ao tratamento de dados pessoais para fins de treinamento de IA generativa, fixando multa diária de cinquenta mil reais em caso de descumprimento. A decisão foi justificada por indícios de infrações à LGPD, especialmente quanto ao uso inadequado de dados pessoais para o treinamento de sistemas de inteligência artificial, com riscos significativos aos direitos e garantias fundamentais, sobretudo para crianças e adolescentes.

Em 10 de julho de 2024, a Meta apresentou um pedido de reconsideração da medida, alegando esforços de adequação às exigências legais. No entanto, a ANPD manteve a suspensão e reiterou a necessidade de a empresa apresentar um plano detalhado de conformidade, acompanhado de um cronograma específico para a implementação de mudanças que garantissem o respeito à legislação vigente.

O desfecho do caso ocorreu em 30 de agosto de 2024, quando a ANPD e a Meta celebraram um acordo que autorizou o uso de sistemas de inteligência artificial pela empresa, desde que em conformidade com as condições estabelecidas no pacto. A Meta demonstrou, à luz do acordo, o cumprimento das exigências impostas pela ANPD, permitindo a retomada de suas operações dentro dos parâmetros legais.

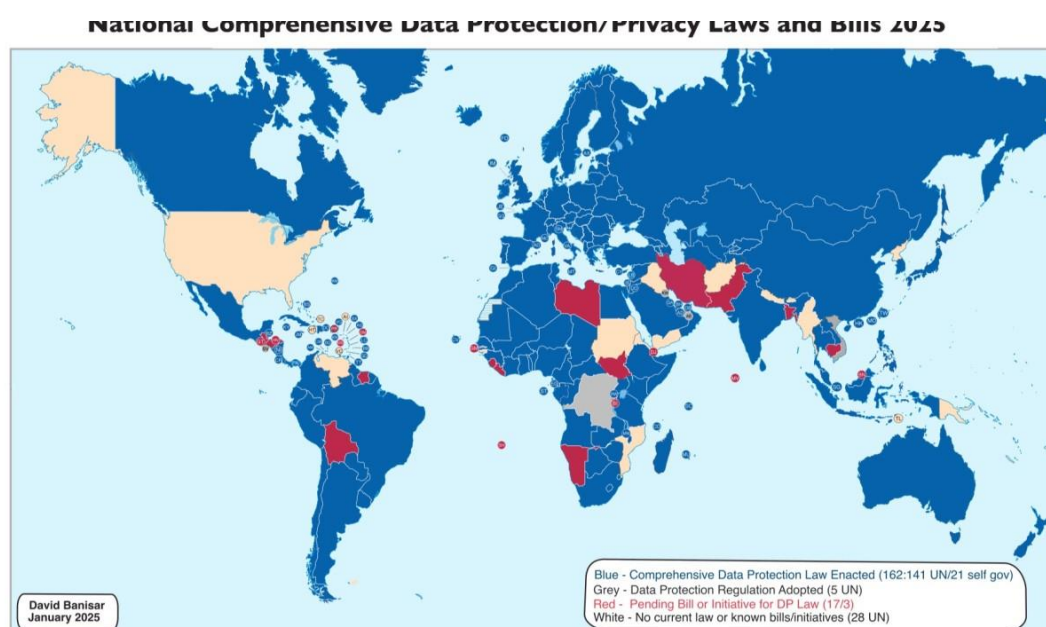
Detalhe, as eleições municipais do Brasil foram realizadas em outubro de 2024. Os candidatos utilizam a Meta em grande escala em suas campanhas políticas e a empresa fatura alto no período eleitoral. Registre-se que em 23 de julho de 2024 foi publicada matéria jornalística na Globo.com que aponta para um aumento de 75% nos gastos de verbas parlamentares destinados ao Facebook⁸. O prazo exíguo do acordo celebrado entre Meta e ANPD perto das eleições é extremamente sugestivo a dúvidas e indagações.

⁸ <https://g1.globo.com/politica/noticia/2024/07/23/deputados-aumentam-em-75percent-gastos-com-facebook-em-um-ano.ghtml> . Acesso em 28 de março de 2025.

A morosidade na fiscalização e consequente aplicação de sanções têm favorecido o tratamento indevido de dados pessoais. A ANPD enfrenta limitações técnicas e operacionais, como falta de recursos humanos, enquanto profissionais de privacidade lutam para mostrar que proteção de dados não é apenas um custo legal. A fragilidade na fiscalização também reduz investimentos empresariais na área, pois empreendedores já têm apetite ao risco.

A figura 2 remete ao mapa de David Banisar sobre as normas de privacidade e proteção de dados no mundo, bem como da adoção de Autoridades Supervisoras em 2025, data da publicação deste artigo.

Figura 2.



Embora seja um mercado relevante, a porcentagem das empresas em conformidade com a LGPD em 2023 era de apenas 36%⁹. Isso o torna como um mercado emergente com boas chances de ser alavancado.

5. CONCLUSÃO

A formação do mercado de privacidade e proteção de dados reflete a transição da sociedade industrial para a era digital, impulsionada pela valorização dos dados

⁹ <https://itforum.com.br/noticias/lcpd-empresas-brasileiras-conformidade/> Acesso em 25 de março de 2025.

peçoais como recurso estratégico e pela promulgação de legislações específicas, como o GDPR na União Europeia e a LGPD no Brasil. Segundo Weber (1994), a dinâmica competitiva entre os agentes econômicos no mercado de privacidade representa uma ação social orientada pela maximização de interesses, em resposta à crescente demanda por segurança e conformidade. No contexto da economia de Nelson e Winter (1982), o mercado de privacidade destaca-se pela adaptação de empresas às exigências legais e tecnológicas, favorecendo aquelas com maior eficiência e capacidade de inovação.

A análise sociológica proposta por Fligstein e Beckert (2006) ressalta que o mercado de privacidade é moldado por instituições e normas que constroem confiança entre provedores e consumidores, enquanto a perspectiva de Kirzner (1973) evidencia a importância do empreendedorismo na identificação de oportunidades e no desenvolvimento de soluções inovadoras no setor. Esses aspectos são cruciais para a compreensão da estruturação do mercado, especialmente no Brasil, onde a consolidação de uma cultura de proteção de dados enfrenta desafios como a desinformação e a falta de maturidade institucional.

A LGPD representou um marco para a regulamentação da privacidade e proteção de dados no Brasil, fomentando a criação de um mercado para serviços especializados, como consultorias jurídicas e tecnológicas, e produtos voltados para a segurança da informação e gestão de conformidade. Contudo, como destaca Banisar (2025), a ausência de reconhecimento internacional pleno, como pela União Europeia, reflete a necessidade de avanços estruturais e culturais.

A atuação da Autoridade Nacional de Proteção de Dados (ANPD) no Brasil reflete avanços importantes na promoção de uma cultura de privacidade e proteção de dados, mas também evidencia desafios significativos, especialmente no que diz respeito à fiscalização e à aplicação de sanções previstas na Lei Geral de Proteção de Dados (LGPD). A atuação nos aspectos educacionais, geração de cultura e a parte regulatória da ANPD são exemplares. No entanto, a falta de recursos humanos para fiscalizar um País de tamanho continental ainda é insuficiente.

Exemplos como a primeira multa pecuniária aplicada à Telekall Infoservice, em 2023, e o caso envolvendo a Meta, em 2024, ilustram a incapacidade da ANPD de agir. A demora na aplicação de sanções, a insuficiência de recursos humanos e a fragilidade na fiscalização têm favorecido práticas questionáveis no uso de dados

pessoais, enquanto a resistência de empresários, aptos aos riscos, em investir em conformidade reforça os desafios enfrentados.

Por fim, o mercado de privacidade e proteção de dados não se limita à conformidade legal; ele constitui um elemento indispensável para o equilíbrio entre inovação tecnológica e respeito aos direitos fundamentais, especialmente em um ambiente marcado por constantes transformações digitais. Assim, investir no fortalecimento desse mercado é essencial para o desenvolvimento sustentável das organizações.

5. REFERÊNCIAS

ARROW, Kenneth J. **The Economic Implications of Learning by Doing**. *Review of Economic Studies*, v. 29, n. 3, p. 155-173, 1996.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **despacho 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 13 mar. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, **despacho decisório disponível em <https://www.in.gov.br/en/web/dou/-/despacho-decisorio-n-1/2024/fis/cgf-540637061>**, acesso em 13 mar. 2025.

BAGNOLI, Vicente. **Pós-Modernidade e o Direito: o fim do começo**. São Paulo: Revista dos Tribunais, 2009.

BANISAR, David. **International Data Protection Day 2025 – Global Update Map**. LinkedIn Pulse, 2 abr. 2025. Disponível em: <https://www.linkedin.com/pulse/international-data-protection-day-2025-global-update-map-banisar-h2ihe/>. Acesso em: 2 abr. 2025.

CASTELLS, Manuel. **A Era da Informação: Economia, Sociedade e Cultura**. Volume 1: A Sociedade em Rede. 6. ed. São Paulo: Paz e Terra, 1999.

COASE, Ronald. **The Nature of the Firm**. *Economica*, v. 4, n. 16, p. 386-405, 1937.

CORRÊA, Caroline Alves Martins Pires. **ANÁLISE DA PROTEÇÃO DA PRIVACIDADE E DOS DADOS PESSOAIS DO USUÁRIO DA CBDC BRASILEIRA 2024**. 113 f. Dissertação (Mestrado em Direito) - Universidade Federal de Minas Gerais, Faculdade de Direito, Belo Horizonte, 2024.

DE MASI, Domenico. **O Ócio Criativo**. 2. ed. Rio de Janeiro: Sextante, 2003.

DE MASI, Domenico (organizador). **A sociedade pós-industrial**. 4ª ed. São Paulo: Editora SENAC São Paulo, 2003.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DOUBLECLICK. **Diretrizes do programa de compradores do Google DoubleClick (AdX)/Admeld**. Disponível em: <https://www.google.com/doubleclick>. Acesso em: 14 set. 2024.

FLIGSTEIN, Neil; BECKERT, Jens. **O mercado como instituição social**. *Journal of Economic Sociology*, 2006.

FORBES. **What Google's 'Don't Be Evil' Slogan Can Teach You About Creating Your Company's Motto**. Disponível em: <https://www.forbes.com>. 13 mar. 2025.

GARTNER. **Cybersecurity Program**. Disponível em: <https://www.gartner.com/en/cybersecurity/topics/cybersecurity-program>. Acesso em: 03 abr. 2025.

JONES, Charles I.; TONETTI, Christopher. **Nonrivalry and the Economics of Data**. *American Economic Review*, v. 110, n. 9, p. 2819-2858, 2020.

KIRZNER, Israel. **Competition and Entrepreneurship**. Chicago: University of Chicago Press, 1973.

LESSIG, Lawrence. **Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity**. New York: Penguin Press, 2004.

LOPES, Giovana Figueiredo Peluso. **INTELIGÊNCIA ARTIFICIAL (IA): Considerações sobre personalidade, imputação e responsabilidade [manuscrito]**. 2020. 160 f. Dissertação (Mestrado em Direito) - Universidade Federal de Minas Gerais, Faculdade de Direito, Belo Horizonte, 2020.

META. **Termos e Políticas de Privacidade**. Disponível em: <https://www.meta.com/privacy>. Acesso em: 13 mar 2025.

NELSON, Richard; WINTER, Sidney. **An evolutionary theory of economic change**. Cambridge: Belknap Press, 1982.

ONU. **Comentário Geral nº 25 sobre os Direitos da Criança no Ambiente Digital**. Disponível em: <https://alana.org.br/wp-content/uploads/2023/10/comentarios-gerais-portugues.pdf>. Acesso em: 20 mar. 2025.

ROHRMANN, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey, 2005.

SCHUMPETER, Joseph. **Teoria do Desenvolvimento Econômico**. São Paulo: Nova Cultural, 1911.

SIQUEIRA, Luiz Felipe Vieira de. **O controle na era digital: legitimação da regulação da internet no Brasil**. 2011. 116 f. Dissertação (Mestrado em Direito Empresarial) - Faculdade de Direito Milton Campos, Nova Lima, 2011.

SNOWDEN. [Filme]. Direção de Oliver Stone. EUA: Open Road Films, 2016. Disponível em: <https://www.primevideo.com>. Acesso em: 13 mar. 2025.

THE GREAT HACK. [Documentário]. Direção de Karim Amer, Jehane Noujaim. EUA: Netflix, 2019. Disponível em: <https://www.netflix.com/title/80117542>. Acesso em: 13 mar. 2025.

THE SOCIAL DILEMMA. [Documentário]. Direção de Jeff Orlowski. EUA: Netflix, 2020. Disponível em: <https://www.netflix.com/br/title/81254224>. Acesso em: 14 mar. 2025.

WEBER, Max. **Economia e Sociedade**. Brasília: Editora Universidade de Brasília, 1994.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power**. New York: *Public Affairs*, 2019.