

**UNIVERSIDADE FEDERAL DE UBERLÂNDIA  
FACULDADE DE DIREITO  
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO**

**JOÃO SOUZA ARAÚJO FILHO**

**A EVOLUÇÃO DAS NORMAS DO DIREITO DIGITAL BRASILEIRO:**  
Da Indústria de Informática à Constitucionalização da Proteção de Dados

UBERLÂNDIA  
2025

**JOÃO SOUZA ARAÚJO FILHO**

**A EVOLUÇÃO DAS NORMAS DO DIREITO DIGITAL BRASILEIRO:**

Da Indústria de Informática à Constitucionalização da Proteção de Dados

Dissertação apresentada como requisito parcial para obtenção do título de Mestre pelo Programa de Pós-graduação em Direito da Universidade Federal de Uberlândia.

Orientador: Prof. Dr. Alexandre Walmott Borges.

UBERLÂNDIA  
2025

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU  
com dados informados pelo(a) próprio(a) autor(a).

A663  
2025

Araújo Filho, João Souza, 1993-  
A EVOLUÇÃO DAS NORMAS DO DIREITO DIGITAL BRASILEIRO  
[recurso eletrônico] : Da Indústria de Informática à  
Constitucionalização da Proteção de Dados / João Souza Araújo  
Filho. - 2025.

Orientador: Prof. Dr. Alexandre Walmott Borges..  
Dissertação (Mestrado) - Universidade Federal de Uberlândia,  
Pós-graduação em Direito.  
Modo de acesso: Internet.  
DOI <http://doi.org/10.14393/ufu.di.2025.440>  
Inclui bibliografia.  
Inclui ilustrações.

1. Direito. I. Borges., Prof. Dr. Alexandre Walmott, 1971-,  
(Orient.). II. Universidade Federal de Uberlândia. Pós-graduação  
em Direito. III. Título.

CDU: 340

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:  
Gizele Cristine Nunes do Couto - CRB6/2091  
Nelson Marcos Ferreira - CRB6/3074



# UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Secretaria da Coordenação do Programa de Pós-Graduação em  
Direito

Av. João Naves de Ávila, 2121, Bloco 3D, Sala 302 - Bairro Santa Mônica, Uberlândia-MG,  
CEP 38400-902

Telefone: 3239-4051 - [mestradodireito@fadir.ufu.br](mailto:mestradodireito@fadir.ufu.br) - [www.cmdip.fadir.ufu.br](http://www.cmdip.fadir.ufu.br)



## ATA DE DEFESA - PÓS-GRADUAÇÃO

Programa de Pós-Graduação em:	Direito				
Defesa de:	Dissertação de Mestrado Acadêmico, número 231, PPGDI				
Data:	Dezoito de julho de dois mil e vinte e cinco	Hora de início:	15:00	Hora de encerramento:	17:00
Matrícula do Discente:	12412DIR006				
Nome do Discente:	João Souza Araújo Filho				
Título do Trabalho:	A evolução das normas do direito digital brasileiro				
Área de concentração:	Direitos e Garantias Fundamentais				
Linha de pesquisa:	Tutela Jurídica e Políticas Públicas				
Projeto de Pesquisa de vinculação:	Efetividade e Devolução de Conceitos Sociais				

Reuniu-se, utilizando tecnologia de comunicação à distância, a Banca Examinadora, designada pelo Colegiado do Programa de Pós-Graduação em Direito, assim composta: Professoras/es Doutoradas/es: Nery dos Santos de Assis - PUC/MG; Ricardo Padovini Pleti Ferreira - UFU; e Alexandre Walmott Borges - UFU - orientador do candidato.

Iniciando os trabalhos o presidente da mesa, Dr. Alexandre Walmott Borges, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao discente a palavra para a exposição do seu trabalho. A duração da apresentação do discente e o tempo de arguição e resposta foram conforme as normas do Programa.

A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o candidato:

**APROVADO.**

Esta defesa faz parte dos requisitos necessários à obtenção do título de Mestre.

O competente diploma será expedido após cumprimento dos demais requisitos, conforme as normas do Programa, a legislação pertinente e a regulamentação interna da UFU.

Neste ato, e para todos os fins de direito, as/os examinadoras/es e o discente autorizam a transmissão ao vivo da atividade. As imagens e vozes não poderão ser divulgadas em nenhuma hipótese, exceto quando autorizadas expressamente pelas/os examinadoras/es e pelo discente. Por ser esta a expressão da vontade, nada haverá a reclamar a título de direitos conexos quanto às imagens e vozes ou quaisquer outros, nos termos firmados na presente.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora e pelo discente.



Documento assinado eletronicamente por **Alexandre Walmott Borges, Presidente**, em 18/07/2025, às 17:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Ricardo Padovini Pleti Ferreira, Professor(a) do Magistério Superior**, em 18/07/2025, às 17:10, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Nery dos Santos de Assis, Usuário Externo**, em 18/07/2025, às 17:16, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **João Souza Araújo Filho, Usuário Externo**, em 18/07/2025, às 17:51, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://www.sei.ufu.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **6523927** e o código CRC **1427687B**.

*À 16ª Turma do Mestrado da Universidade Federal de Uberlândia*

## AGRADECIMENTOS

Encerrar uma jornada é, de certa forma, reencontrar o início. Ao olhar para trás, cada passo se revela mais significativo do que eu jamais poderia imaginar. Esta dissertação não é apenas o fruto de um percurso acadêmico, mas o reflexo de uma travessia que moldou tanto meu intelecto quanto meu caráter.

Em cada conquista da minha vida, nunca estive sozinho. Ao meu lado estiveram aqueles que foram parte essencial desta caminhada, e é com profundo reconhecimento que externo minha gratidão a todos que, de uma forma ou outra, me estenderam a mão.

A Deus, meu sustento nos dias de dúvida, alento nas madrugadas silenciosas de insônia e fonte inesgotável de esperança quando as forças me faltaram. Meu sustento mesmo nos momentos de ceticismo e quando minha estrutura foi abalada. Não teria chegado até esse momento sem a fé.

À Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG), agradeço o apoio essencial que viabilizou a realização desta pesquisa.

Aos meus pais, cuja presença silenciosa e amorosa sempre foi o alicerce sobre o qual construí minha vida. São o meu Norte e a razão primordial do meu esforço cotidiano.

À minha esposa, Isabela Maria Silva Souza, minha companheira nesta e em todas as jornadas. És meu porto seguro, meu alicerce e meu refúgio.

Às minhas pequenas e barulhentas filhas, Helena e Cecília, que me ensinaram a enxergar a vida com leveza, alegria e pureza.

Ao meu estimado orientador, Alexandre Walmott Borges, que, antes mesmo de ser meu orientador, foi meu amigo. Ao senhor, a minha mais sincera gratidão por sua generosidade e paciência. Obrigado por compartilhar seu tempo e por me transmitir ensinamentos que vão além dos livros. O levarei para a vida.

Aos meus mentores, que sempre admirei pessoal e profissionalmente, Adelino José de Carvalho Dias e Ronaldo Silva Dimas.

A todos os meus colegas do mestrado que me ajudaram de todas as formas possíveis: Ana Carolina, Anna Júlia, Bruna, Bárbara, Caio, Carolina, Feliciano, Felipe, Grazielly, João Flávio, João Doreto, Leonardo, Luciano, Luiza, Marco, Raíssa, Samuel, Thais, Victor e Vinicius. Mencionar cada um de vocês aqui é um gesto de reconhecimento e retribuição, um retrato coletivo da minha imensa gratidão pela convivência e admiração que tenho por todos.

Pneu furou  
Acenda o farol, acenda o farol  
Se alguém ligou  
Acenda o farol, acenda o farol

Se alguém ligou, minha senhora  
Se alguém lhe amou e foi-se embora

Você pode se encontrar  
Você deve se ajudar  
E viver tranquilamente  
Sentindo disposto

Pneu furou  
Acenda o farol, acenda o farol (...)

*Acenda o farol, Tim Maia*



## RESUMO

A presente dissertação realiza uma análise histórico-normativa da evolução do Direito Digital no Brasil, com ênfase na consolidação legislativa e nos desafios contemporâneos da regulação tecnológica. Parte-se da hipótese de que o marco jurídico brasileiro se estruturou em fases sucessivas — regulação de *hardware*, *software* e dados — refletindo um modelo predominantemente reativo, setorial e fragmentado, frente às transformações aceleradas da sociedade da informação. A investigação adota abordagem metodológica qualitativa, de natureza descritiva e analítica, por meio da triangulação entre análise documental de normas, exame jurisprudencial e revisão doutrinária nacional e internacional. O estudo percorre três eixos evolutivos: (i) a formação do setor de informática sob políticas protecionistas e a atuação de órgãos como a CAPRE e a SEI; (ii) a transição normativa para o reconhecimento jurídico do software e os desafios da propriedade intelectual na década de 1990; e (iii) a consolidação do marco regulatório digital, com destaque para o Marco Civil da Internet e a Lei Geral de Proteção de Dados, culminando na elevação do direito à proteção de dados ao patamar de direito fundamental pela Emenda Constitucional nº 115/2022. A pesquisa evidencia a permanência de lacunas regulatórias em setores estratégicos como inteligência artificial e plataformas digitais, ao mesmo tempo em que problematiza a fragmentação normativa, a ausência de governança coordenada e os limites de uma atuação institucional reativa. Constata-se que, embora o ordenamento jurídico tenha amadurecido em temas como proteção de dados e segurança cibernética, ainda carece de um regime normativo sistêmico, harmônico, integrado e prospectivo, capaz de enfrentar os desafios jurídicos da era algorítmica. O trabalho contribui para o debate sobre os impasses da regulação estatal tradicional e propõe a construção de um paradigma normativo transversal, fundamentado pelos princípios.

**Palavras-chave:** Direito Digital; Regulação Tecnológica; Proteção de Dados; Fragmentação Normativa.

## ABSTRACT

This dissertation presents a historical-normative analysis of the evolution of Digital Law in Brazil, with emphasis on legislative consolidation and the contemporary challenges of technological regulation. It is based on the hypothesis that the Brazilian legal framework has developed in successive phases—regulation of hardware, software, and data—reflecting a predominantly reactive, sector-based, and fragmented model in response to the rapid transformations of the information society. The research adopts a qualitative methodological approach, both descriptive and analytical in nature, through the triangulation of legal norm analysis, jurisprudential review, and national and international legal scholarship. The study is structured around three evolutionary axes: (i) the formation of the computing sector under protectionist policies and the roles of institutions such as CAPRE and SEI; (ii) the normative transition toward the legal recognition of software and the challenges of intellectual property in the 1990s; and (iii) the consolidation of the digital regulatory framework, notably with the Civil Rights Framework for the Internet and the General Data Protection Law, culminating in the elevation of data protection to the status of a fundamental right through Constitutional Amendment No. 115/2022. The research highlights the persistence of regulatory gaps in strategic areas such as artificial intelligence and digital platforms, while also problematizing normative fragmentation, the lack of coordinated governance, and the limitations of a reactive institutional posture. It concludes that, although the legal framework has matured in areas such as data protection and cybersecurity, it still lacks a systemic, coherent, integrated, and forward-looking normative regime capable of addressing the legal challenges of the algorithmic age. The study contributes to the broader debate on the impasses of traditional state regulation and advocates for the construction of a transversal regulatory paradigm grounded in constitutional principles.

**Keywords:** Digital Law; Technological Regulation; Data Protection; Normative Fragmentation.

## LISTA DE ABREVIATURAS

**ABES:** Associação Brasileira das Empresas de *Software*  
**ABINEE:** Associação Brasileira da Indústria Elétrica e Eletrônica  
**ABNT:** Associação Brasileira de Normas Técnicas  
**ADPF:** Arguição de Descumprimento de Preceito Fundamental  
**ADI:** Ação Direta de Inconstitucionalidade  
**AED:** Análise Econômica do Direito  
**AIR:** Análise de Impacto Regulatório  
**Anvisa:** Agência Nacional de Vigilância Sanitária  
**ANATEL:** Agência Nacional de Telecomunicações  
**ANPD:** Autoridade Nacional de Proteção de Dados  
**ASSESPRO:** Associação das Empresas de Processamento de Dados  
**CADE:** Conselho Administrativo de Defesa Econômica  
**CAPRE:** Coordenação das Atividades de Processamento Eletrônico de Dados  
**CDC:** Código de Defesa do Consumidor  
**CF:** Constituição Federal  
**C&T:** Ciência e Tecnologia  
**CMN:** Conselho Monetário Nacional  
**CONIN:** Conselho Nacional de Informática e Automação  
**CTI:** Centro Tecnológico para Informática  
**DAE:** Departamento de Águas e Esgotos  
**DDoS:** Distributed Denial of Service (Ataque de Negação de Serviço Distribuído)  
**E-Ciber:** Estratégia Nacional de Segurança Cibernética  
**EC:** Emenda Constitucional  
**EBIA:** Estratégia Brasileira de Inteligência Artificial  
**FAI:** Fundo para Atividades de Informática  
**FisDigi:** Fundo de Fiscalização Digital  
**GEDICE:** Grupo Executivo para o Desenvolvimento da Indústria de Computadores Eletrônicos  
**GTE:** Grupo de Trabalho Especial  
**HC:** Habeas Corpus  
**IA:** Inteligência Artificial  
**IIC:** Invenções Implementadas por Computador

**ICP-Brasil:** Infraestrutura de Chaves Públicas Brasileira

**ICTs:** Instituições Científicas e Tecnológicas

**IDC:** International Data Corporation

**IG:** Indicação Geográfica

**ITI:** Instituto Nacional de Tecnologia da Informação

**INPI:** Instituto Nacional da Propriedade Industrial

**LAI:** Lei de Acesso à Informação

**LGPD:** Lei Geral de Proteção de Dados Pessoais

**LPI:** Lei de Propriedade Industrial

**MCI:** Marco Civil da Internet

**MCTIC:** Ministério da Ciência, Tecnologia, Inovações e Comunicações

**MLG:** Marco Legal dos Games

**NBR:** Norma Brasileira

**P&D:** Pesquisa e Desenvolvimento

**P&D+I:** Pesquisa, Desenvolvimento e Inovação

**PC:** Personal Computer (Computador Pessoal)

**PIX:** Sistema de Pagamentos Instantâneos do Brasil

**PL:** Projeto de Lei

**PNI:** Política Nacional de Informática

**PNSI:** Política Nacional de Segurança da Informação

**PPB:** Processo Produtivo Básico

**REsp:** Recurso Especial

**SBPC:** Sociedade Brasileira para o Progresso da Ciência

**SEI:** Secretaria Especial de Informática

**SETAD/MCTI:** Secretaria de Transformação Digital do Ministério da Ciência, Tecnologia e Inovações

**SNCTI:** Sistema Nacional de Ciência, Tecnologia e Inovação

**STF:** Supremo Tribunal Federal

**STJ:** Superior Tribunal de Justiça

**TCP/IP:** Transmission Control Protocol/Internet Protocol

**TIC:** Tecnologia da Informação e Comunicação

**TJ:** Tribunal de Justiça

**UNIVAC:** Universal Automatic Computer

## LISTA DE TABELAS

<b>Tabela 1</b> - Elementos centrais da computação .....	14
<b>Tabela 2</b> - Quadro da evolução normativa .....	122
<b>Tabela 3</b> - Agrupamento das normas por assuntos .....	124
<b>Tabela 4</b> - Eventos – Linha Evolutiva.....	126

# SUMÁRIO

<b>1</b>	<b>CONCEITOS E BASES DA PESQUISA .....</b>	<b>14</b>
<b>2</b>	<b>INTRODUÇÃO .....</b>	<b>18</b>
<b>3</b>	<b>NORMAS DA INDÚSTRIA DE INFORMÁTICA NO BRASIL.....</b>	<b>22</b>
3.1	A indústria da informática .....	27
3.2	A lei da reserva de mercado.....	30
<b>4</b>	<b>NORMAS SOBRE HARDWARE E SOFTWARE .....</b>	<b>35</b>
<b>5</b>	<b>MARCO REGULATÓRIO DIGITAL .....</b>	<b>43</b>
5.1	Internet.....	47
5.2	Proteção de Dados .....	52
5.3	Segurança Cibernética .....	59
5.4	Jogos Eletrônicos.....	62
5.5	Regulação do Poder Econômico Digital.....	66
5.6	Inteligência Artificial.....	68
5.7	Plataformas Digitais .....	78
<b>6</b>	<b>O DIREITO DIGITAL À LUZ DA CONSTITUIÇÃO.....</b>	<b>84</b>
6.1	A centralidade dos princípios na regulação digital.....	87
6.2	Elevação da proteção de dados à direito fundamental.....	96
<b>7</b>	<b>CONSIDERAÇÕES FINAIS.....</b>	<b>103</b>
<b>8</b>	<b>REFERÊNCIAS .....</b>	<b>106</b>
<b>9</b>	<b>ANEXOS .....</b>	<b>122</b>

1      **CONCEITOS E BASES DA PESQUISA**

Aqui serão inseridos os principais conceitos, informações e bases teóricas:

- a) Direito eletrônico e direito digital;
- b) Abordagem cronológica e evolutiva;
- c) Listagem dos conceitos extrajurídicos e a inserção no sistema normativo;
- d) Universo eletrônico e digital;
- e) Disciplinas coligadas: computação e informática;
- f) Estruturas físicas e lógicas – *hardware* e *software*;
- g) Dados;
- h) IA e outras ferramentas, equipamentos e mecanismos de informática e de dados;
- i) IA e inteligência natural (outras categorias).

**Tabela 1** - Elementos centrais da computação

COMPONENTE	FUNÇÃO PRINCIPAL E DETALHES
Unidade Central de Processamento (CPU)	Processamento e controle: O cérebro da operação. Executa instruções, gerencia o fluxo de dados, realiza cálculos e coordena tarefas. Agendamento de tarefas: Aloca recursos para garantir multitarefa eficiente.
Unidade de Processamento Gráfico (GPU)	Renderização gráfica: Processa dados visuais para jogos, vídeos e modelagem 3D. Processamento paralelo: Executa múltiplos cálculos simultaneamente, ideal para IA e simulações científicas.
Unidade de Processamento Neural (NPU)	Computação específica para IA: Acelera tarefas de IA como reconhecimento de imagem/fala e processamento de linguagem natural. Integração de sistema: Trabalha com a CPU/GPU para otimizar a eficiência geral do sistema.
Memória Unificada (RAM)	Armazenamento temporário de dados: Guarda dados e instruções em uso ativo para acesso rápido. Essencial para multitarefa. Alocação dinâmica de recursos: Permite que a CPU e a GPU compartilhem memória, reduzindo a duplicação de dados.
Armazenamento (SSD)	Armazenamento persistente: Guarda o sistema operacional, apps e arquivos permanentemente, mesmo com o computador desligado. Desempenho de alta velocidade: Permite inicialização e carregamento rápidos de programas e arquivos.
Tela (Display)	Saída visual: Apresenta a interface, textos e imagens ao usuário através de pixels. Feedback do sistema: Exibe notificações e outros elementos interativos do <i>software</i> .

Energia (Power)	Fonte de energia: Fornece energia para todos os componentes através de baterias e carregadores. Otimização de desempenho: Equilibra o consumo de energia para melhorar a vida útil da bateria e reduzir o calor.
Portas (Ports)	Conectividade de periféricos: Pontos de conexão física para dispositivos externos (monitores, HDs externos etc.). Transferência de dados: Suporta protocolos como USB-C e <i>Thunderbolt</i> (interface de conexão física super-rápida (usando conector USB-C) para conectar periféricos externos como monitores, disco) para troca rápida de dados e energia
Teclado e Painel de controle (Keyboard and Control Panel)	Entrada do usuário: Permitem a inserção de texto, comandos e gestos. Controle da interface: Facilitam a navegação no sistema operacional e nos aplicativos.
Sistema de Resfriamento (Cooling System)	Gerenciamento térmico: Dissipa o calor gerado pela CPU e GPU para evitar superaquecimento. Sustentabilidade de desempenho: Permite que os componentes operem em alta performance sem superaquecer.
Câmera e Áudio (Camera and Audio)	Entrada e saída de mídia: Capturam e reproduzem som e imagem para videochamadas, gravações e consumo de mídia. Experiência de alta qualidade: Integram microfones e alto-falantes para som claro e imagem nítida.
Sistema Operacional (Operating System)	Gerenciamento de recursos: Gerencia o <i>hardware</i> do computador (CPU, memória, armazenamento) e aloca recursos para os aplicativos. Lida com multitarefa e garante a estabilidade do sistema. Interface do usuário: Fornece uma Interface Gráfica do Usuário (GUI) ou linha de comando (CLI) para permitir a interação entre os usuários e o sistema. Gerenciamento de processos: Supervisiona a execução de todos os programas e processos, garantindo a estabilidade e segurança do sistema.
Núcleo (Kernel)	Funcionalidade central do sistema: Atua como o núcleo do sistema operacional, responsável por tarefas de baixo nível como gerenciamento de memória, agendamento de processos e comunicação de <i>hardware</i> . Camada de abstração: Fornece uma camada padronizada para o <i>software</i> interagir com o <i>hardware</i> , ocultando as complexidades dos diferentes <i>hardwares</i> .
Drivers (Programas de computador)	Camada de interface de dispositivo: Permitem que o sistema operacional se comunique com dispositivos de <i>hardware</i> específicos (ex: placas de vídeo, impressoras, adaptadores de rede). Operações específicas de <i>hardware</i> : Fornecem ao sistema operacional um controle detalhado sobre o dispositivo, traduzindo comandos genéricos em ações específicas do <i>hardware</i> .



Sistema de Arquivos (File System)	Gerenciamento de dados: Define como os dados são armazenados e recuperados em discos e outros dispositivos de armazenamento. Fornece acesso estruturado aos dados para aplicações e usuários. Integridade dos dados: Garante a precisão e consistência dos dados através de técnicas como <i>journaling</i> (registro por diário) e controle de acesso.
Recursos de Segurança (Security Features)	Controle de acesso: Implementa permissões para usuários e processos, controlando quem pode acessar e modificar arquivos e recursos do sistema. Proteção de dados: Utiliza criptografia e métodos de armazenamento seguro para proteger dados sensíveis contra acesso não autorizado e violações. Monitoramento do sistema: Detecta e responde a atividades suspeitas e vulnerabilidades, tomando as medidas necessárias para manter a integridade do sistema.
Suporte a Aplicações (Application Support)	Ambiente de execução: Fornece a infraestrutura e os serviços necessários para que as aplicações de <i>software</i> funcionem (ex: alocação de memória, E/S de arquivos, renderização de gráficos). Camada de compatibilidade: Garante que o <i>software</i> funcione em diferentes ambientes de <i>hardware</i> e <i>software</i> .
Multitarefa (Multitasking)	Execução concorrente: Permite que múltiplos aplicativos e processos rodem "simultaneamente", alocando dinamicamente o tempo da CPU. Agendamento de processos: Os processos são organizados e executados com base em prioridade e requisitos do sistema.
Rede (Networking)	Conectividade e comunicação: Fornece as interfaces de rede e os protocolos necessários para permitir a comunicação entre computadores em uma rede e na internet. Protocolos de transporte: Implementa padrões como TCP/IP para transmissão de dados confiável entre dispositivos.
Virtualização (Virtualization)	Compartilhamento de recursos: Suporta a criação e o gerenciamento de máquinas virtuais (VMs), permitindo que múltiplos sistemas operacionais e serviços rodem em um único <i>hardware</i> físico. Abstração em nível de sistema: Permite que sistemas ou aplicações isoladas acessem recursos de <i>hardware</i> compartilhados sem interferir uns nos outros. Alocação de recursos: Permite que o <i>hardware</i> (CPU, armazenamento) seja alocado dinamicamente para instâncias virtuais conforme a necessidade.
Recursos de Acessibilidade (Accessibility Features)	Recursos personalizáveis: Permitem que os usuários modifiquem a interface do sistema, o comportamento e os métodos de entrada para atender às suas necessidades pessoais.

A compreensão dos fundamentos técnicos da computação constitui requisito essencial para a análise dos desafios jurídicos inerentes à era digital. O escopo do Direito Digital transcende a mera abordagem de normas abstratas, demandando o conhecimento aprofundado da operação de sistemas computacionais. A observação das estruturas físicas e lógicas desses sistemas revela sua influência direta na formulação e aplicação das normas jurídicas.

A arquitetura computacional, englobando componentes como Unidades Centrais de Processamento (CPUs), Unidades de Processamento Gráfico (GPUs) e Unidades de Processamento Neural (NPU), configura um ecossistema integrado. Esta integração processa a natureza dos dados, que são atualmente considerados ativos jurídicos, com implicações que se estendem da privacidade à segurança nacional. Adicionalmente, o sistema operacional desempenha função central na gestão de recursos, na aplicação de políticas de segurança e na intermediação da relação entre o usuário e o *hardware*.

O avanço da inteligência artificial (IA), aliado à utilização de *hardware* especializado, tem gerado tensões normativas inéditas. Questões como a atribuição de responsabilidade por decisões proferidas por sistemas autônomos e a definição de autoria em ambientes permeados por agentes não humanos emergem como desafios. Tais indagações exigem a reformulações de categorias clássicas do Direito, ante o dinamismo tecnológico que supera a celeridade da produção normativa.

Recursos como a virtualização e a acessibilidade não se restringem a funcionalidades operacionais; configuram instrumentos para a efetivação de direitos fundamentais. Neste contexto, a tecnologia não apresenta caráter neutro, possuindo a capacidade de ampliar ou restringir liberdades individuais e coletivas.

O presente capítulo estabelece os conceitos fundamentais que sustentam a análise normativa a ser desenvolvida nos capítulos subsequentes. A articulação entre Direito e tecnologia permite demonstrar que a evolução regulatória brasileira, abarcando desde a proteção de *hardware* até o tratamento de dados e a IA, demanda uma abordagem sistêmica. Esta abordagem visa a equilibrar a inovação tecnológica, a segurança jurídica e a proteção de direitos na era algorítmica.

## 2 INTRODUÇÃO

A presente dissertação analisa a evolução do marco regulatório brasileiro no ambiente digital, mapeando seu desenvolvimento em resposta às transformações tecnológicas e sociais. O presente estudo foca na adaptação da legislação nacional aos desafios do avanço tecnológico, desde a incipiência normativa inicial até a configuração de um sistema regulatório mais complexo.

Compreendemos, como um dos principais problemas identificados no curso da investigação, a dificuldade crônica do sistema jurídico em acompanhar o ritmo acelerado das inovações. Defasagem que se manifesta na desarticulação entre normas setoriais, nos conflitos entre soberania estatal e poder das plataformas digitais, e nos crescentes desafios para garantir direitos, de forma geral, no ambiente digital.

Diante desse cenário, a pesquisa busca responder: como as normas jurídicas brasileiras evoluíram para regulamentar o Direito Digital? Dessa indagação, almejamos compreender como a herança protecionista condicionou a atual fragmentação regulatória das tecnologias emergentes e quais os desafios jurídicos ainda persistem.

Assim, o estudo delimita-se à investigação da trajetória histórica da legislação brasileira voltada à regulação dos ambientes digitais e eletrônicos, percorrendo desde os primeiros dispositivos normativos sobre informática, surgidos na década de 1960, até a elevação da proteção de dados a direito fundamental. Trata-se, portanto, de uma análise cronológica e evolutiva dos cinquenta anos da legislação brasileira de regulação dos ambientes e sistemas digitais e eletrônicos.

A hipótese é que a trajetória legislativa seguiu uma lógica evolutiva, partindo da regulação de *hardware* e desenvolvimento industrial de informática, avançando para o *software* e, posteriormente, consolidando-se em normas abrangentes sobre proteção de dados, segurança cibernética e outras inovações.

Essa progressão, impulsionada pela "Revolução do PC", demandou novas regulações em privacidade, segurança e economia digital. Contudo, persistem desafios como fragmentação normativa, insuficiência de regras para tecnologias emergentes e a necessidade de harmonização.

O objetivo geral é examinar a trajetória do marco regulatório digital no Brasil, das origens aos desafios futuros. Já os objetivos específicos incluem: descrever a fase inicial de regulação focada em *hardware*; avaliar detalhadamente o Marco Civil da Internet (MCI) e a Lei

Geral de Proteção de Dados (LGPD); e mapear desafios atuais, como a fragmentação normativa e a regulação incipiente de IA e jogos eletrônicos.

Como a pesquisa se debruça em análise de normas, metodologicamente a pesquisa adota abordagem qualitativa, descritiva e analítica, caracterizando-se como estudo jurídico exploratório. O procedimento se baseou em um estudo documental de fontes primárias: legislação, da política de informática à LGPD e MCI, e secundárias: doutrina nacional e internacional, decisões judiciais predominantemente do STF.

O exame seguiu perspectiva cronológica e temática, mapeando desde o surgimento da indústria de informática no Brasil até as regulamentações atuais sobre proteção de dados, segurança cibernética, internet, jogos eletrônicos e IA. O método envolveu a coleta sistemática de normas ao longo do tempo, contextualizando cada período regulatório em relação às transformações tecnológicas e sociais subjacentes, construindo uma linha evolutiva da regulação de *hardware* ao *software* e às legislações recentes.

Dessarte, buscou-se traçar a evolução cronológica do setor, analisar como políticas governamentais refletem mudanças socioeconômicas e tecnológicas, identificar avanços e lacunas nas regulações vigentes e destacar desafios contemporâneos em direitos digitais, segurança da informação e inovação tecnológica.

Quanto a estrutura da pesquisa, esta dissertação organiza-se em quatro eixos analíticos: em primeiro momento, realiza-se uma abordagem da construção histórica da indústria de informática no Brasil, examinando marcos como a importação do UNIVAC 120 e a implementação da política de reserva de mercado. Procedeu-se à análise dos impactos dessa política na industrialização tecnológica nacional e à discussão dos dilemas inerentes à tensão entre protecionismo e competitividade setorial.

Na sequência, dedica-se à exploração da base constitucional e jurisprudencial do Direito Digital brasileiro. Explora-se o processo de reinterpretação de princípios jurídicos tradicionais pelo STF para a sua aplicação no ambiente digital, com especial atenção aos desdobramentos introduzidos pela Emenda Constitucional (EC) nº 115/2022.

Posteriormente, examina-se os regimes jurídicos distintos aplicáveis a *hardware* e *software*, com base na Lei de Direitos Autorais, na Lei do *Software* e na Lei de Propriedade Industrial (LPI). A investigação enfoca os desafios contemporâneos no âmbito da propriedade intelectual no contexto digital, incluindo questões relativas a *softwares* e jogos eletrônicos.

E, por fim, analisa-se a edificação do marco regulatório digital no Brasil, abrangendo legislações como as proposições legislativas sobre IA, proteção de dados e as normativas sobre segurança cibernética. Conclui-se a verificação com uma discussão crítica acerca dos limites

da regulação jurídica e setorial, particularmente no que concerne às plataformas digitais e aos sistemas de inteligência artificial.

Na organização da pesquisa, utilizou-se de material bibliográfico, incluindo doutrina, artigos, livros e revistas, para contextualizar a evolução normativa. Este material foi fundamental para apresentar a introdução das normas, seus objetivos primordiais, os pontos de maior relevância e as alterações mais impactantes ou importantes em termos de avanço normativo.

Especificamente, obras doutrinárias, artigos acadêmicos, livros e decisões judiciais constituíram a base para fornecer o suporte teórico necessário, contextualizar o objeto de estudo, permitir uma análise crítica aprofundada e oferecer diferentes perspectivas sobre o tema. Dessa maneira, o estudo deste acervo permitiu ir além da mera descrição legal, possibilitando a observação e interpretação da evolução normativa, com um consequente aprofundamento conceitual e avaliativo.

Empreendeu-se a incorporação de trechos de diretrizes normativas no desenvolvimento textual com objetivo subsidiar a elucidação de disposições regulamentares consideradas pertinentes à compreensão do objeto de estudo. A inserção desses fragmentos visa a fundamentação e a objetividade da exposição.

Já as notas de rodapé foram empregadas com diversas funções: prover informações adicionais ou explicativas, contextualizar debates ou entendimentos, apontar material de apoio e aprofundar discussões pontuais do texto principal. As notas referenciam fontes variadas, incluindo leis específicas, decretos, portarias, artigos acadêmicos, relatórios, livros e decisões judiciais relevantes.

Dessa forma, as informações contidas nas notas complementam o corpo do texto sem interromper o fluxo de leitura, além de incorporar análises críticas de especialistas sobre as normas estudadas. Adicionalmente, essas notas servem para dar o necessário suporte acadêmico às constatações apresentadas, detalhando as fontes e enriquecendo a compreensão do tema com camadas adicionais de informação e contexto.

Para sistematizar as informações sobre a evolução normativa brasileira em Direito Digital, foram incluídas tabelas ao final do trabalho, com a finalidade de oferecer um resumo estruturado e de fácil consulta das normas centrais abordadas, facilitando a visualização da trajetória legislativa e a identificação por assunto.

A tabela nº 1 aponta os elementos centrais da computação, servindo como uma espécie de glossário. Já a tabela nº 2 apresenta um quadro da evolução normativa, listando as normas por ano e categorizando-as, proporcionando uma visão cronológica das primeiras

regulamentações. A tabela nº 3 agrupa as normas por categorias temáticas, listando as leis e decretos pertinentes sob cada agrupamento. Por derradeiro, a tabela nº 4 expõe os eventos em linha evolutiva.

Conquanto o foco principal resida na descrição da trajetória evolutiva, a análise incorpora a discussão de desafios persistentes e projeta perspectivas para o aprimoramento contínuo do marco regulatório digital.

A pergunta que ainda permanece é: como regular o digital sem engessar o futuro? Essa questão, longe de ser meramente teórica, define o destino democrático nacional e da economia na era algorítmica, exigindo equilíbrio entre inovação, segurança jurídica e proteção aos direitos fundamentais.

### 3 NORMAS DA INDÚSTRIA DE INFORMÁTICA NO BRASIL

A indústria de informática no Brasil teve seu marco inicial em 1957, com a importação do UNIVAC120, primeiro computador instalado no país, adquirido pelo Departamento de Águas e Esgotos de São Paulo para modernizar cálculos administrativos (IT Forum, 2022).<sup>1</sup> Na década de 1960, o setor ainda era incipiente, com políticas que favoreciam a entrada de multinacionais como a *International Business Machines* (IBM) (Asianometry, 2023).

A introdução da computação eletrônica identifica o Censo estadunidense de 1950 como evento catalisador para o desenvolvimento do mercado comercial de computadores, destacando-se o emprego do equipamento UNIVAC.

No contexto brasileiro, a observação dos registros aponta a importação pioneira de um computador, modelo UNIVAC, pela prefeitura de São Paulo no final da década de 1950, destinado a tarefas administrativas. O período subsequente registrou instalações adicionais em São Paulo e no Rio de Janeiro, majoritariamente para aplicações em rotinas administrativas (Pereira; Marinho, 2014, p. 1).<sup>2</sup>

Foi em 1957 que o “Computador Automático Universal”, ou Univac120, fabricado pelo grupo norte-americano Remington Rand, foi instalado no país e se tornou o primeiro computador em solo nacional. A máquina foi adquirida pela prefeitura de São Paulo e utilizada pelo Departamento de Águas e Esgotos (DAE), com o objetivo de modernizar os cálculos do órgão (IT Forum, 2022).

Nos anos 1970, o governo brasileiro adotou uma postura protecionista, buscando desenvolver uma indústria nacional<sup>3</sup> por meio de medidas como restrições à importação, reserva

<sup>1</sup> Durante as décadas de 1950 e 1960, observa-se a introdução de *mainframes* no Brasil por empresas como IBM e Burroughs, voltados a grandes corporações e órgãos públicos; a indústria nacional de computadores é analisada por Marcelino (2003), enquanto a política brasileira de informática entre 1970 e 1984 é objeto do estudo de Lopes (1986); os debates legislativos em torno das leis de informática de 1984, 1991, 2001 e 2004 são abordados por Cukierman, Castro e Alves (2012); quanto ao conceito de software, “o *software* lato sensu é o conjunto de 3 elementos distintos: o programa de computador, a descrição do programa e o material de apoio. A palavra expressão, empregada pelo legislador torna defeituoso o conceito trazido pelo referido artigo de lei. Tanto a descrição do programa de computador como o material de apoio se inserem na categoria das obras protegidas pelo Direito Autoral, não reclamando proteção de lei específica, pois são obras científicas expressas em linguagem humana e destinadas à sua informação e auxílio. Os programas de computador, por outro lado, reclamam a aplicação de lei específica. Isto porque sua natureza jurídica não se amolda ao regime protetivo autoral, exigindo a observância de suas peculiaridades” (Viegas, 2020); para uma leitura de contexto, ver IT Forum (2022) sobre empresas emblemáticas da TI brasileira, Asianometry (2023) sobre a política de proteção à indústria nacional, a ABINEE (2023) sobre o setor de informática e eletrônicos no país e Tecnoblog (2019) quanto aos custos da limitação das importações. IT Forum. Dia da Informática: 6 empresas que marcaram a história da TI no Brasil. Disponível em: <https://itforum.com.br/noticias/6-empresas-historia-informatica-brasil/>. Acesso em: 23 maio 2025.

<sup>2</sup> PEREIRA, L.; MARINHO, MGS. O cérebro eletrônico do IBGE: análise sobre os impactos da importação de um computador eletrônico para a realização do Censo de 1960. Anais III SHIALC, p. 1-8, 2014.

<sup>3</sup> ASIANOMETRY. Brazil Tried to Protect Its Computer Industry. 2023. (23min25s). Disponível em: <https://www.youtube.com/watch?v=brOtbWIViWM>. Acesso em: 19 maio 2025.

de mercado e incentivos fiscais para produção local de *hardware* e *software*<sup>4</sup> (Vargas, 1996, p. 73).<sup>5</sup>

Na realidade, a história da evolução da indústria nacional de computadores comporta duas fases: a primeira onde predominava o livre comércio e a importação de equipamentos de empresas fabricantes multinacionais, que predominou até quase a metade da década de 1970; e a segunda, a partir de 1974, quando se estabeleceram as bases e diretrizes de uma política nacional de informática, e os meios de ação para implementá-la, com o contingenciamento das importações e a reserva de mercado na faixa dos minicomputadores (Marcelino, 1983, p. 90).<sup>6</sup>

Essa mudança estratégica foi impulsionada pela criação da Coordenação das Atividades de Processamento Eletrônico de Dados (CAPRE) em 1972, órgão responsável por racionalizar o uso de computadores no setor público e, posteriormente, por assessorar a formulação de políticas industriais. A CAPRE desempenhava as seguintes atribuições:

a) organizar e manter atualizado um cadastro detalhado do parque computacional privado e governamental, no que se refere a equipamentos, programas e grau de utilização das instalações; b) opinar sobre compras e locações de equipamentos, pretendidas por órgãos e entidades da Administração Pública Federal Direta e Indireta, principalmente no que tange ao dimensionamento, em função das suas necessidades atuais e futuras de eventuais ociosidade de equipamentos de outras instituições que possam atender, total ou parcialmente, às referidas necessidades; c) propor medidas pendentes à formulação de uma política de financiamento governamental ao setor privado, para a atividade de processamento de dados; d) coordenar programas de treinamento em todos os níveis das técnicas computacionais, fazendo uso dos recursos já existentes nas universidades, escolas e centros de pesquisa (Brasil, 1972).

Uma verificação empreendida por Rodrigues (2018, p. 90) acerca dos registros discursivos permite identificar a recorrência do tema da independência e do desenvolvimento de tecnologia nacional no debate à época. Não obstante, a concretização desse objetivo revelava-se intrinsecamente complexa, conforme delineado pela autora em sua exposição: “como se demonstrou também no caso brasileiro, a conquista da independência em informática

<sup>4</sup> A terminologia jurídica relativa a “*software*” exige delimitação conceitual: para Viegas (2020), o software em sentido lato compreende “o conjunto de 3 elementos distintos: o programa de computador, a descrição do programa e o material de apoio”, sendo que a expressão adotada pelo legislador torna “defeituoso o conceito trazido pelo referido artigo de lei”; segundo o autor, tanto a descrição quanto o material de apoio enquadram-se como obras protegidas pelo Direito Autoral, por serem “obras científicas expressas em linguagem humana e destinadas à sua informação e auxílio”, ao passo que os programas de computador, dada sua natureza jurídica própria, “reclamam a aplicação de lei específica”, pois “não se amoldam ao regime protetivo autoral, exigindo a observância de suas peculiaridades”. VIEGAS, Cláudia Mara de Almeida Rabelo. Proteção jurídica do *software*. JusBrasil, 2020. Disponível em: <https://www.jusbrasil.com.br/artigos/propriedade-industrial-protecaojuridica-do-software/760054078>. Acesso em: 12 maio 2025.

<sup>5</sup> VARGAS, Milton. História da Informática no Brasil. Rio de Janeiro: Campus, 1996.

<sup>6</sup> MARCELINO, Gileno Fernandes. A indústria nacional de computadores. Revista de Administração de Empresas, São Paulo, v. 43, n. 2, p. 8-20, 2003. Disponível em: <https://www.revistas.usp.br/rausp/article/download/166948/159505/393477>. Acesso em: 12 maio 2025



(hoje se diria Tecnologia da Informação), com uma indústria nacional, não era uma coisa simples”.<sup>7</sup>

Em 1976, a CAPRE<sup>8</sup> ampliou suas atribuições, regulando importações e incentivando a produção nacional de minicomputadores, um mercado em expansão à época. Em 1977, cinco empresas, incluindo a estatal COBRA e algumas empresas privadas, foram selecionadas para atuar nesse segmento, segundo Marcelino (1983, p. 90):

Conforme já assinalado, até o fim dos anos 60, a informática quase inexistia como setor da economia brasileira. Ela começou a se corporificar em 1971, com a criação do GTE — Grupo de Trabalho Especial, e posteriormente, em 1972, com a CAPRE — Coordenação das Atividades de Processamento Eletrônico de Dados, uma autarquia criada para racionalizar o uso de computadores e periféricos, especialmente para os órgãos governamentais. Em 1976, a CAPRE teve sua competência ampliada, passando a assessorar a Presidência da República na formulação de um modelo de política industrial de informática. Suas atribuições foram ampliadas no sentido de regular as importações de equipamentos de processamento de dados, peças e componentes. Levando em conta o rápido desenvolvimento tecnológico da indústria nacional de microeletrônica, foi escolhido o novo mercado de minicomputadores, ainda não existente no país, como reserva de mercado, com restrições à importação. Em 1977, foi realizada uma concorrência e selecionadas 5 empresas: a COBRA (estatal); a LABO, a SID, a EDISA e a SISCO, privadas.<sup>9</sup>

A política protecionista se consolidou na Lei nº 7.232/1984<sup>10</sup> (Lei da Reserva de Mercado de Informática) visava proteger a indústria nacional, limitando a concorrência estrangeira. Essa medida, porém, gerou controvérsias. Enquanto setores nacionalistas e militares defendiam a soberania tecnológica, críticos argumentavam que o isolamento prejudicava a inovação e a competitividade:

<sup>7</sup> Texto de Silvia Helena Vianna Rodrigues intitulado “Como a defesa de uma indústria brasileira de informática ganhou as páginas da grande imprensa” publicado no Simpósio de História da Informática na América Latina e Caribe (5.: 2018: Rio de Janeiro). TAROUCO, Liane Margarida Rockenbach; MUSSE, Jussara Issa. Uma história da evolução das redes de computadores no Brasil. Simpósio de História da Informática na América Latina e Caribe (5.: 2018: Rio de Janeiro). Memórias do V Simpósio de História da Informática na América Latina e Caribe. Rio de Janeiro: UFRJ, 2018, 2018. RODRIGUES, Silvia Helena. Como a defesa de uma indústria brasileira de informática ganhou as páginas da grande imprensa. In: TAROUCO, Liane Margarida Rockenbach; MUSSE, Jussara Issa. Memórias do V Simpósio de História da Informática na América Latina e Caribe. Rio de Janeiro: UFRJ, 2018.

<sup>8</sup> O artigo 9º da Lei nº 7.232/84 institui a reserva de mercado para bens de informática visando “assegurar adequados níveis de proteção às empresas nacionais, enquanto não estiverem consolidadas e aptas a competir no mercado internacional (...)”; nesse sentido, Cukierman (2014, p. 17) observa que a resolução da CAPRE de 1976 já estabelecia tal reserva para minicomputadores, com foco na preservação da soberania tecnológica e estruturação de um mercado interno, sendo que a publicidade teve papel relevante ao enfatizar a origem nacional dos produtos. CUKIERMAN, H. L. A publicidade dos minicomputadores made in Brazil ea experiência da reserva de mercado dos anos 70/80. In: Proc. III Simposio de Historia de la Informática de América Latina y el Caribe. 2014. p. 17-28.

<sup>9</sup> MARCELINO, Gileno Fernandes. A indústria nacional de computadores. Revista de Administração, v. 18, n. 2, p. 90-95, 1983.

<sup>10</sup> BRASIL. Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/Leis/L7232.htm](https://www.planalto.gov.br/ccivil_03/Leis/L7232.htm). Acesso em: 19 maio 2025.

Em 30/7/1984, o Poder Executivo submeteu ao Congresso Nacional o Projeto de Lei no 10/1984, que tratava da Política Nacional de Informática (PNI). O texto proposto consolidava o Estado como principal agente econômico do setor, condicionando o mercado a seus interesses, especialmente com a adoção de reserva de mercado. Houve forte mobilização parlamentar sobre o tema, formando-se o que Campos (1994, p. 1.091) chamou de “bizarro pacto MolotovRibbentrop na eletrônica digital”. A coalizão a favor da lei unia os militares da SEI, temerosos pela perda do poder político – e que viam na informática uma fonte de poder –, e as esquerdas, seduzidas pela ideia nacionalista contra o imperialismo tecnológico das multinacionais, além dos empresários paulistas, encantados com a ideia de um mercado protegido e subvencionado.

A COBRA Computadores, criada em 1974 como empresa estatal, destacou-se na produção de *hardware*, mas, com o fim da reserva em 1991, enfrentou dificuldades diante da abertura econômica, migrando posteriormente para serviços de TI (Tecnoblog, 2019).

A Secretaria Especial de Informática, organismo ligado à Presidência da República e criado em outubro de 1979, decidiu, em 6 de agosto de 1980, abrir a fabricação de pequenos computadores no Brasil para duas multinacionais, a Hewlett Packard, produzindo microprocessadores, e a IBM, produzindo algo na fronteira entre minis e médios computadores. Como a tecnologia, nesta área, avança sempre no sentido de melhor performance com menor preço, é óbvio a virtual queda da reserva de mercado para minicomputadores no país (Helena, 1980, p. 75).<sup>11</sup>

Paralelamente, o desenvolvimento de *software*<sup>12</sup>, inicialmente tratado como secundário, ganhou relevância nos anos 1980 com a popularização dos microcomputadores e o surgimento de empresas como Microsiga (atual TOTVS) e Itautech. Apesar dos desafios, como a escassez de mão de obra qualificada, esse período marcou a transição de um modelo centrado no *hardware* para outro que valorizava a inovação em programas e sistemas (Cukierman; Castro; Alves, 2012, p. 3):

O objetivo da reserva de mercado, vigente no país desde 1976, seria basicamente o de defender as indústrias brasileiras de *hardware*, que à época não tinham condições de enfrentar a concorrência estrangeira, até que pudessem “caminhar com as próprias pernas”. Mais ainda, o domínio da tecnologia da informação foi tratado nos debates

<sup>11</sup> HELENA, Silvia. A indústria de computadores: evolução das decisões governamentais. Revista de Administração Pública, v. 14, n. 4, p. 73 a 109-73 a 109, 1980.

<sup>12</sup> Segundo Maxim e Pressman (2021, p. 57), “o *software* abrange uma vasta gama de aplicações”, sendo a engenharia de software desafiada em sete frentes principais: o *Software* de Sistema oferece suporte a outros programas, desde compiladores a sistemas operacionais e drivers; o de Aplicação atende a demandas específicas de negócios, processando dados e apoiando decisões; o Engenharia/Científico lida com cálculos avançados em áreas como astronomia e meteorologia; o Embarcado controla funções específicas de dispositivos, do micro-ondas a veículos; o de Linha de Produtos reutiliza componentes para diferentes mercados; as Aplicações Web e Mobile operam em redes, incluindo navegadores, serviços em nuvem e apps móveis; e o de Inteligência Artificial aplica heurísticas em tarefas complexas, como robótica e aprendizado de máquina, refletindo a continuidade evolutiva e o esforço coletivo da engenharia de software entre gerações. MAXIM, Bruce R.; PRESSMAN, Roger S. Engenharia de Software: uma abordagem profissional. Porto Alegre:[sn], 2021.

como assunto estratégico e fundamental para o desenvolvimento tecnológico do país. Alguns palestrantes foram além e relacionaram a informática como sendo um importante instrumento para preservar a soberania nacional, caso do Professor Clodovaldo Pavan, então presidente da SBPC – Sociedade Brasileira para o Progresso da Ciência, e destacaram o poder da informática sobre as decisões que regeriam o rumo do país, caso de Eduardo Guy, então presidente da ASSESPRO – Associação das Empresas de Processamento de Dados.<sup>13</sup>

A chamada "Revolução do PC", impulsionada pelo microprocessador e pela difusão de computadores pessoais, redefiniu o cenário tecnológico global. No Brasil, esse movimento acelerou a democratização do acesso à informática, consolidou novas indústrias (como a de *software* e jogos) e transformou práticas sociais e econômicas. Com isso, nas décadas de 1970 e 1980 foram decisivas para a formação de um ecossistema digital nacional, ainda que marcado por contradições entre protecionismo e a necessidade de integração com o mercado global.

A narrativa a seguir segue uma ordem cronológica, começando com as primeiras tentativas de comercializar o computador eletrônico no final dos anos 1940 e terminando em meados dos anos 1990, quando as estações de trabalho pessoais em rede se tornaram comuns. Identifiquei vários pontos de virada importantes, que recebem a análise mais detalhada. Eles incluem a transformação do computador no final dos anos 1940, de um instrumento especializado para a ciência em um produto comercial, o surgimento de pequenos sistemas no final dos anos 1960, o advento da computação pessoal nos anos 1970 e a disseminação das redes após 1985 (Ceruzzi, 2003, p.6).<sup>14</sup> (tradução livre)

Conforme estudo realizado por Cunha, Zeferino e Vianna (2018, p. 500) o Brasil observou um processo de acentuado desenvolvimento no setor de informática entre o final da década de 1970 e 1984. Em cenário de crise econômica, a política protecionista adotada impulsionou a indústria nacional, registrando taxas de crescimento anual da ordem de 30%.<sup>15</sup>

Como resultado, essa expansão manifestou-se na oferta de mais de 40 modelos de microcomputadores no mercado interno e na ampla circulação de publicações especializadas, a exemplo da revista *Microsistemas*, cuja tiragem evoluiu de 10 mil exemplares em 1981 para

<sup>13</sup> CUKIERMAN, Henrique Luiz; CASTRO, Rachel Gonçalves de; ALVES, Luiz Augusto da Silva. Os debates parlamentares das leis de informática (1984, 1991, 2001, 2004). I SIMPÓSIO DE HISTÓRIA DA INFORMÁTICA NA ALC. Medellín, 2012.

<sup>14</sup> Texto original: "The narrative that follows is chronological, beginning with the first attempts to commercialize the electronic computer in the late 1940s and ending in the mid-1990s, as networked personal workstations became common. I have identified several major turning points, and these get the closest scrutiny. They include the computer's transformation in the late 1940s from a specialized instrument for science to a commercial product, the emergence of small systems in the late 1960s, the advent of personal computing in the 1970s, and the spread of networking after 1985." CERUZZI, Paul E. *A History of Modern Computing*. 2. ed. Cambridge, MA: MIT Press, 2003.

<sup>15</sup> VIANNA, Marcelo; ZEFERINO, PRISCILA Yasmin da Rocha; CUNHA, Laura Castro da. "O futuro nunca esteve tão presente em sua vida": o microcomputador na sociedade brasileira através da revista *Micro Sistemas* (1981-1983). *MoExp-Mostra de Ensino, Extensão e Pesquisa do Campus Osório*, v. 1, n. 1, p. 1-1, 2018.

45 mil em 1983, evidenciando a dinamização do mercado no período examinado (Cunha; Zeferino; Vianna, 2018, p. 501).

### 3.1 A indústria da informática

As primeiras regulamentações do setor de informática no Brasil emergiram na década de 1960, em um contexto de modernização administrativa e tentativa de estruturar a política tecnológica nacional.

Em 1967, o Decreto-Lei nº 200<sup>16</sup> modernizou a gestão pública, facilitando a adoção de computadores por órgãos governamentais, ainda que sem foco específico em tecnologia. Embora não se trate propriamente de uma norma voltada ao tratamento da informática, a reforma administrativa contribuiu para a ampliação do uso de computadores nos órgãos da administração pública, ao simplificar e promover a modernização dos processos governamentais (Brasil, 1967).

Um marco significativo foi o Decreto nº 70.370/1972<sup>17</sup>, que instituiu a Comissão de Coordenação das Atividades de Processamento Eletrônico, vinculada ao Ministério do Planejamento. Suas atribuições incluíam:

- a) organizar e manter atualizado um cadastro detalhado do parque computacional privado e governamental, no que se refere a equipamentos, programas e grau de utilização das instalações; b) opinar sobre compras e locações de equipamentos, pretendidas por órgãos e entidades da Administração Pública Federal Direta e Indireta, principalmente no que tange ao dimensionamento, em função das suas necessidades atuais e futuras de eventuais ociosidade de equipamentos de outras instituições que possam atender, total ou parcialmente, às referidas necessidades; c) propor medidas pendentes à formulação de uma política de financiamento governamental ao setor privado, para a atividade de processamento de dados; d) coordenar programas de treinamento em todos os níveis das técnicas computacionais, fazendo uso dos recursos já existentes nas universidades, escolas e centros de pesquisa (Brasil, 1972).

---

<sup>16</sup>O decreto representou marco na reforma administrativa do regime militar ao promover a descentralização da gestão pública por meio da criação de entidades com maior autonomia, porém sob controle estatal, impacto que perdura na configuração atual do setor público; os §§ 1º a 3º regulam aspectos como controle acionário, natureza administrativa e formalização jurídica, consolidando a estrutura institucional da reforma de 1967. BRASIL. Decreto-lei nº 200, de 25 de fevereiro de 1967. Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Diário Oficial da União, Brasília, DF, 27 fev. 1967. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del0200.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm). Acesso: 19 maio 2025.

<sup>17</sup> BRASIL. Decreto nº 70.370, de 5 de abril de 1972. Cria a Comissão de Coordenação das Atividades de Processamento Eletrônico, e dá outras providências. Diário Oficial da União, Brasília, DF, 13 jan. 2025. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1970-1979/decreto-70370-5-abril-1972-418827-publicacaooriginal-1-pe.html>. Acesso em: 19 maio 2025.

Essa estrutura reforçou o papel do Estado no planejamento tecnológico, alinhado à estratégia de substituição de importações. Os incentivos fiscais ganharam força com o Decreto-Lei nº 1.209/1972<sup>18</sup>, que beneficiava empresas investidoras em produção nacional de *hardware* e *software* (Brasil, 1972).

Na segunda metade dos anos 1970, portarias interministeriais como as de nº 10/1975<sup>19</sup> e 291/1976<sup>20</sup> consolidaram o controle sobre importações e a concessão de incentivos para componentes eletrônicos. Em 1979, a Portaria nº 361<sup>21</sup> atualizou as regras de importação, enquanto o Decreto nº 84.067/1979<sup>22</sup> substituiu a CAPRE pela Secretaria Especial de Informática (SEI), subordinada ao Conselho de Segurança Nacional.

A SEI assumiu funções estratégicas, como assessorar na formulação da PNI e fiscalizar atividades tecnológicas. Isso refletiu em um modelo de desenvolvimento tecnológico centralizador, protecionista e alinhado aos interesses de segurança nacional:

Art. 1º É criada, como órgão complementar do Conselho de Segurança Nacional, a Secretaria Especial de Informática, SEI, com a finalidade de assessorar na formulação da Política Nacional de Informática (PNI) e coordenar sua execução, como órgão superior de orientação, planejamento, supervisão e fiscalização, tendo em vista, especialmente, o desenvolvimento científico e tecnológico no setor. Art. 2º As atividades de informática serão organizadas sob a forma de Sistema, a que serão integradas todas as unidades organizacionais, de qualquer grau, incumbidas especificamente das mencionadas atividades. Art. 3º A Secretaria Especial de

<sup>18</sup> BRASIL. Decreto-Lei nº 1.209, de 2 de outubro de 1972. Concede incentivos fiscais para programas especiais de desenvolvimento e dá outras providências. Diário Oficial da União, Brasília, DF, 3 out. 1972. Disponível em: <https://www2.camara.leg.br/legin/fed/declei/1970-1979/decreto-lei-1209-28-fevereiro-1972-375353-publicacaooriginal-1-pe.html>. Acesso: 19 maio 2025.

<sup>19</sup> BRASIL. Ministério da Fazenda. Ministério do Planejamento e Coordenação Geral. Portaria Interministerial nº 10, de 17 de janeiro de 1975. Estabelece normas para a concessão de incentivos fiscais à produção de componentes eletrônicos. Diário Oficial da União, Brasília, DF, 20 jan. 1975.

<sup>20</sup> BRASIL. Comissão de Coordenação das Atividades de Processamento Eletrônico. Portaria nº 291, de 21 de maio de 1976. Dispõe sobre a importação de equipamentos de informática. Diário Oficial da União, Brasília, DF, 24 maio 1976. BRASIL. Secretaria Especial de Informática. Portaria nº 361, de 3 de agosto de 1979. Dispõe sobre a importação de bens de informática. Diário Oficial da União, Brasília, DF, 6 ago. 1979.

<sup>21</sup> BRASIL. Ministério da Fazenda. Ministério do Planejamento e Coordenação Geral. Portaria Interministerial nº 10, de 17 de janeiro de 1975. Estabelece normas para a concessão de incentivos fiscais à produção de componentes eletrônicos. Diário Oficial da União, Brasília, DF, 20 jan. 1975. BRASIL. Comissão de Coordenação das Atividades de Processamento Eletrônico. Portaria nº 291, de 21 de maio de 1976. Dispõe sobre a importação de equipamentos de informática. Diário Oficial da União, Brasília, DF, 24 maio 1976. BRASIL. Secretaria Especial de Informática. Portaria nº 361, de 3 de agosto de 1979. Dispõe sobre a importação de bens de informática. Diário Oficial da União, Brasília, DF, 6 ago. 1979.

<sup>22</sup> O Decreto nº 84.067/1979 marca a política tecnológica do regime militar ao instituir a Secretaria Especial de Informática (SEI), vinculada ao Conselho de Segurança Nacional, com a missão de coordenar a Política Nacional de Informática (PNI) e promover a autonomia tecnológica brasileira por meio da normatização, fiscalização e incentivo à pesquisa, extinguindo a CAPRE, centralizando decisões e garantindo sustentação financeira via Fundo para Atividades de Informática (FAI). BRASIL. Decreto nº 84.067, de 2 de outubro de 1979. Cria a Secretaria Especial de Informática e dá outras providências. Diário Oficial da União, Brasília, DF, 3 out. 1979. Disponível em:

Informática será chefiada por um Secretário nomeado pelo Presidente da República, por indicação do Secretário-Geral do Conselho de Segurança Nacional (Brasil, 1979).

O Decreto nº 84.067/1979 serviu de alicerce para a Lei da Informática, que consolidou a reserva de mercado por alguns anos. Contudo, essa medida foi considerada um entrave ao desenvolvimento tecnológico do Brasil, pois o isolou de inovações internacionais. Logo, embora tenha contribuído para a estruturação do setor no país, a SEI também limitou a abertura ao mercado internacional, criando um ambiente controlado pelo Estado (Mendes, 2022, p. 15).

As diretrizes até aqui levantadas prepararam o terreno para a Lei nº 7.232/1984, que instituiu a reserva de mercado por oito anos, consolidando o protecionismo industrial. O projeto, aprovado após intensos debates no Congresso, refletia uma coalizão heterogênea: militares da SEI, setores nacionalistas e empresários paulistas, todos interessados em proteger a indústria nacional.

(...) foi aprovada a Lei da Informática, nos termos em que proposta pelo Governo. Mediante a Lei nº 7.232/1984, instituiu-se a política de informática brasileira, calcada na reserva de mercado de oito anos para empresas de capital nacional na área de produção de bens e serviços relacionados à informática. Para Campos (1991b, p. 37), essas restrições nada mais foram do que a marginalização do Brasil na corrida tecnológica (Mendes, 2022, p. 15).

Deveras, a Lei nº 7.232/1984 estabeleceu a política de informática brasileira, instituindo uma reserva de mercado de quase uma década para empresas nacionais no setor. Essa medida, contudo, foi interpretada por analistas como uma marginalização tecnológica do país.

Segundo Mendes (2022, p. 16), em resposta à nova legislação da política de informática brasileira, Roberto Campos<sup>23</sup> apresentou uma arguição de inconstitucionalidade contra a lei em questão e seus atos normativos complementares. A representação, sustentada por pareceres jurídicos especializados, foi submetida ao Procurador-Geral da República. Na fundamentação da ação, argumentou-se que a norma violava diversos princípios constitucionais, como a liberdade de iniciativa, o direito adquirido, a isonomia e a liberdade de empresa, além de afrontar os princípios jurídicos da legalidade e da indelegabilidade de funções.<sup>24</sup>

Entre as décadas de 1960 e 1980 a política brasileira de informática seguiu um modelo centralizador e protecionista, que, embora tenha impulsionado a indústria nascente, acabou por

<sup>23</sup> Apelidado de “o constituinte profeta” por Gilmar Ferreira Mendes, Roberto Campos (1917–2001), economista, diplomata e político liberal, destacou-se pela defesa do desenvolvimento tecnológico, da abertura de mercado e da formulação de um marco jurídico compatível com a era digital, antecipando debates sobre regulação tecnológica e liberdade econômica, sendo suas críticas a políticas restritivas influentes em reformas posteriores no setor. MENDES, Gilmar Ferreira. Roberto Campos: o Constituinte profeta. 2022.

<sup>24</sup> MENDES, Gilmar Ferreira. Roberto Campos: o Constituinte profeta. 2022.

isolar o país tecnologicamente, comprometendo sua competitividade e inovação. Esse arranjo normativo, marcado por contradições entre o intervencionismo estatal e os princípios da livre iniciativa, revelou-se, com o tempo, mais um entrave do que um catalisador do progresso tecnológico.

### 3.2 A lei da reserva de mercado

A Lei da Reserva de Mercado de Informática, representou o ápice da política protecionista brasileira no setor tecnológico. Promulgada em um contexto de busca pela soberania industrial, a legislação estabeleceu barreiras à importação de produtos de informática e reservou segmentos estratégicos do mercado para empresas nacionais. Dessa lei<sup>25</sup>, constata-se sua origem na necessidade de superar a dependência tecnológica do Brasil e edificar capacidade nacional no setor, percebido como estratégico para o desenvolvimento multifacetado (Brasil, 1984).

Em seu artigo 1º criou estruturas fundamentais como o Conselho Nacional de Informática e Automação (CONIN) e os Distritos de Exportação de Informática, além de instituir o Plano Nacional de Informática e Automação, nestes termos:

Art. 1º Esta Lei estabelece princípios, objetivos e diretrizes da Política Nacional de Informática, seus fins e mecanismos de formulação, cria o Conselho Nacional de Informática e Automação - CONIN, dispõe sobre a Secretaria Especial de Informática - SEI, cria os Distritos de Exportação de Informática, autoriza a criação da Fundação Centro Tecnológico para Informática - CTI, institui o Plano Nacional de Informática e Automação e o Fundo Especial de Informática e Automação (Brasil, 1984).

O cerne da lei estava em seu artigo 4º, que definia os instrumentos da Política Nacional de Informática. Além de definir os pilares da política estatal brasileira para a informática na década de 1980, combinando protecionismo, incentivos industriais e capacitação tecnológica, a PNI tinha como objetivo proteger, desenvolver e consolidar a indústria nacional de

---

<sup>25</sup> O artigo 2º da Lei da Reserva de Mercado visava à capacitação nacional em informática por meio de intervenção estatal, restrição à importação e controle sobre empresas estrangeiras, protegendo a indústria doméstica centrada em hardware; sua execução, contudo, revelou foco limitado, com negligência a setores emergentes como inteligência artificial e computação em nuvem, baixo investimento em microeletrônica e software, e ausência de política exportadora, resultando em uma indústria defasada, tecnologicamente dependente e pouco competitiva, evidenciando os limites de um protecionismo descolado da evolução tecnológica e da lógica global, sendo a posterior Lei nº 8.248/91 indicativa de inflexão rumo à abertura ao revogar dispositivos da Lei nº 7.232/84. BRASIL. Lei nº 13.874, de 20 de setembro de 2019. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/Leis/L7232.htm](https://www.planalto.gov.br/ccivil_03/Leis/L7232.htm). Acesso em: 19 maio 2025.

informática, reduzindo a dependência tecnológica do país e fomentando a capacitação local, conforme a literalidade de seus incisos:

I - o estímulo ao crescimento das atividades de informática de modo compatível com o desenvolvimento do País; II - a institucionalização de normas e padrões de homologação e certificação de qualidade de produtos e serviços de informática; III - a mobilização e a aplicação coordenadas de recursos financeiros públicos destinados ao fomento das atividades de informática; IV - o aperfeiçoamento das formas de cooperação internacional para o esforço de capacitação do País; V - a formação, o treinamento e o aperfeiçoamento de recursos humanos para o setor; VI - a instituição de regime especial de concessão de incentivos tributários e financeiros, em favor de empresas nacionais, destinados ao crescimento das atividades de informática; VII - as penalidades administrativas pela inobservância de preceitos desta Lei e regulamento; VIII - o controle das importações de bens e serviços de informática por 8 (oito) anos a contar da publicação desta Lei; IX - a padronização de protocolo de comunicação entre sistemas de tratamento da informação; e X - o estabelecimento de programas específicos para o fomento das atividades de informática, pelas instituições financeiras estatais (Brasil, 1984).

A implantação da reserva de mercado no setor de informática produziu efeitos ambíguos. Evidenciou-se, por um lado, o fomento ao desenvolvimento de empresas nacionais, como a COBRA Computadores, e a consequente formação de um ecossistema industrial doméstico. Por outro lado, observaram-se críticas relativas à reduzida competitividade dos produtos nacionais, à elevação dos preços e à crescente defasagem tecnológica em comparação ao cenário internacional. A abertura econômica, que culminou no término da reserva em 1991, expôs tais vulnerabilidades e impulsionou a reestruturação do setor (Cukierman; Castro; Alves, 2012, p. 7).

Essas limitações tornaram-se evidentes com a abertura econômica dos anos 1990, que levou ao fim do regime da reserva em 1992. E um dos pilares da lei era o Processo Produtivo Básico<sup>26</sup>, que obrigava empresas beneficiadas por incentivos fiscais a cumprir metas de nacionalização na fabricação de bens de informática. Além disso, as empresas deveriam investir um percentual do faturamento em pesquisa e desenvolvimento (P&D), visando estimular a inovação local. A lei também previa controle estatal sobre a importação e exportação de

---

<sup>26</sup> O Processo Produtivo Básico (PPB), instituído pela Lei nº 8.387/91, define o conjunto mínimo de etapas fabris a serem realizadas em território nacional para caracterizar a industrialização de um bem, sendo seu cumprimento requisito para a concessão de incentivos fiscais; embora concebido sob o governo Collor, sua formalização inicial ocorreu na gestão Itamar Franco, em contexto de abertura econômica e revogação da reserva de mercado de informática em 1992, marcando o abandono de políticas protecionistas, sendo sua regulamentação operacionalizada por Portarias Interministeriais conjuntas do Ministério da Economia e do MCTIC. BRASIL. Lei nº 8.387, de 30 de dezembro de 1991. Dá nova redação ao § 1º do art. 3º aos arts. 7º e 9º do Decreto-Lei nº 288, de 28 de fevereiro de 1967, ao caput do art. 37 do Decreto-Lei nº 1.455, de 7 de abril de 1976 e ao art. 10 da Lei nº 2.145, de 29 de dezembro de 1953, e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/L8387.htm](https://www.planalto.gov.br/ccivil_03/leis/L8387.htm). Acesso em: 7 de abr. de 2025.



componentes eletrônicos, como semicondutores, e regulamentava a exploração de bases de dados (Brasil, 1984).

A transição para um novo modelo ocorreu com a promulgação da Lei nº 8.248/1991, que manteve incentivos à indústria nacional, mas abandonou o protecionismo radical. Essa mudança passou por alterações significativas entre 2001 e 2019, sendo a mais recente promovida pela Lei nº 13.969/2018. Como consequência, os benefícios passaram a estar condicionados a exigências específicas, como investimentos mínimos em pesquisa e desenvolvimento (P&D) e a integração com instituições acadêmicas, atualizando, assim, os objetivos originais de capacitação tecnológica. Esse novo direcionamento pode ser visto no trecho abaixo:

Para fazer jus aos benefícios previstos nesta lei, as empresas que tenham como finalidade a produção de bens e serviços de informática deverão aplicar, anualmente, no mínimo 5% (cinco por cento) do seu faturamento bruto no mercado interno decorrente da comercialização de bens e serviços de informática (deduzidos os tributos correspondentes a tais comercializações), em atividades de pesquisas e desenvolvimento a serem realizadas no País, conforme projeto elaborado pelas próprias empresas. Parágrafo único. No mínimo 2% (dois por cento) do faturamento bruto mencionado no caput deste artigo deverão ser aplicados em convênio com centros ou institutos de pesquisa ou entidades brasileiras de ensino, oficiais ou reconhecidas (Brasil, 1991).

As modificações posteriores<sup>27</sup> da Lei nº 8.248/1991 feita pela Lei nº 13.969/2019<sup>28</sup>, adaptaram o marco legal às novas demandas da indústria 4.0<sup>29</sup>, substituindo benefícios fiscais por créditos financeiros:

---

<sup>27</sup> As intervenções normativas precedentes incluem a Lei nº 10.176/2001 e a Lei nº 11.484/2007, que promoveram alterações e acréscimos à Lei nº 8.248/1991. Adicionalmente, regulamentações por meio de decretos, como o Decreto nº 5.906/2006 e o Decreto nº 10.356/2020, complementam o arcabouço normativo, estabelecendo diretrizes para a operacionalização dos dispositivos legais: BRASIL. Lei nº 10.176, de 11 de janeiro de 2001. Altera dispositivos da Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a Política Nacional de Informática. Diário Oficial da União, Brasília, DF, 12 jan. 2001. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/leis\\_2001/110176.htm](http://www.planalto.gov.br/ccivil_03/leis/leis_2001/110176.htm). Acesso em: 12 maio 2025. Lei nº 11.484, de 31 de maio de 2007. Altera e acresce dispositivos à Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a Política Nacional de Informática. Diário Oficial da União, Brasília, DF, 1 jun. 2007. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2007-2010/2007/Lei/L11484.htm](http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2007/Lei/L11484.htm). Acesso em: 12 maio 2025. BRASIL. Decreto nº 5.906, de 26 de setembro de 2006. Regulamenta a Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a Política Nacional de Informática. Diário Oficial da União, Brasília, DF, 27 set. 2006. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2004-2006/2006/decreto/d5906.htm](http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5906.htm). Acesso em: 12 maio 2025. BRASIL. Decreto nº 10.356, de 20 de maio de 2020. Regulamenta a Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a Política Nacional de Informática. Diário Oficial da União, Brasília, DF, 21 maio 2020. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/Decreto/D10356.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Decreto/D10356.htm). Acesso em: 12 maio 2025.

<sup>28</sup> BRASIL. Lei nº 13.969, de 26 de dezembro de 2019. Altera a Lei nº 8.248, de 23 de outubro de 1991, para dispor sobre a nova forma de concessão dos incentivos fiscais de que trata a referida Lei. Diário Oficial da União, Brasília, DF, 27 dez. 2019. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/L13969.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13969.htm). Acesso em: 12 maio 2025.

<sup>29</sup> Para Pereira e Simoneto (2018, p. 1-3), diferente das revoluções anteriores, é estudada enquanto ocorre, não a posteriori a Indústria 4.0 é a Quarta Revolução Industrial, caracterizada pela integração de tecnologias digitais.

Art. 2º As pessoas jurídicas fabricantes de bens de tecnologias da informação e comunicação que investirem em atividades de pesquisa, desenvolvimento e inovação, que cumprirem o processo produtivo básico e que estiverem habilitadas nos termos da Lei nº 8.248, de 23 de outubro de 1991, farão jus, até 31 de dezembro de 2029, ao crédito financeiro referido no art. 4º da referida Lei (Brasil, 2019).

Apesar de seu caráter temporário, a experiência da reserva de mercado proporcionou uma contribuição importante, além de demonstrar a capacidade do Estado brasileiro em formular políticas setoriais complexas, criou bases normativas que permitiram a adaptação contínua do setor às transformações tecnológicas. Todavia, se a reserva de mercado fortaleceu empresas nacionais, seu desmonte em 1991 expôs vulnerabilidades que ecoam na atual regulação de software, conforme veremos no próximo capítulo.

Contudo, se partimos para uma análise um pouco mais crítica, podemos dizer que devido a uma combinação de políticas equivocadas e problemas estruturais, o Brasil não se tornou tão bem-sucedido à época na área de TI. Na década de 1980, a reserva de mercado isolou a indústria nacional da inovação global, limitando-a à produção de clones defasados de computadores, como os PCs da COBRA, sem desenvolvimento tecnológico genuíno<sup>30</sup>.

Em 1985, a indústria de computadores brasileira era relativamente desenvolvida, apesar de não poder ser comparada à indústria norte-americana, por exemplo (Evans 1995: 160-168). Apesar de produzir hardware de maneira competente, a indústria não conseguia competir com a nova tecnologia (Luzio, 1996, p. 121). Tendo apoio dos maiores bancos e grupos empresariais, o país podia se gabar de possuir e fazer computadores, mas não podia dizer que a tecnologia fosse nacional. Os “clones” de PC montados no Brasil dominavam a maior parte do mercado de computadores pessoais com praticamente nenhuma tecnologia nativa empregada; as empresas brasileiras tinham um claro incentivo para serem “caronas” da política de proteção e de engenharia reversa, enquanto usavam essa proteção para exportar (Borges, 2011, p. 83).

As empresas dependiam de subsídios estatais e não investiam em pesquisa própria, exemplificado pelo sistema SOX, criado tardiamente pela COBRA quando já estava à beira da falência. Esse modelo despertou retaliações internacionais, como as sanções dos EUA em 1985, expondo a fragilidade econômica e diplomática do país.

---

Seu núcleo são fábricas inteligentes, onde humanos e máquinas interagem em redes colaborativas, permitindo autonomia decisória, customização em massa (produtos personalizados com eficiência industrial) e gestão de alta complexidade. PEREIRA, Adriano; SIMONETTO, Eugênio de Oliveira. Indústria 4.0: conceitos e perspectivas para o Brasil. Revista da Universidade Vale do Rio Verde, v. 16, n. 1, 2018.

<sup>30</sup> BORGES, Bruno de Moura. Desenvolvimento e Autonomia: O Brasil e a Tecnologia de Informação em Perspectiva Histórica Comparada. Desigualdade & Diversidade, n. 8, p. 77-100, 2011.

Segundo Borges (2011, p. 85) nos anos 1990, “a política havia se tornado impossível comercialmente e acabava representando, na prática, uma barreira à inovação e um caminho de estagnação.” O fim abrupto da reserva levou à desindustrialização do setor: empresas nacionais foram compradas por multinacionais ou faliram, reduzindo a atividade à mera montagem de *hardware* importado. O Estado abandonou políticas setoriais estratégicas, privatizando ativos como a Embratel sem criar alternativas para inovação (Borges, 2011, p. 84).

Programas como "Computador para Todos" falharam ao ignorar a cultura tecnológica vigente (73% dos usuários substituíam Linux por Windows pirata). Em síntese, o país oscilou entre protecionismo isolacionista e liberalização desordenada, sem políticas de Estado contínuas que integrassem educação, investimento em pesquisa e inserção global inteligente, condenando-se à dependência tecnológica (Borges, 2011, p. 97).

Por conseguinte, com base no estudo de Borges (2011), podemos assentar diagnóstico de que a falha brasileira na tentativa de alavancar o setor de informática se deu pelo fato de priorizar modelos anacrônicos (protecionismo nos anos 80, liberalização abrupta nos anos 90) sem articular educação, inovação e mercado.

A trajetória da indústria de informática no Brasil revela uma dinâmica complexa, marcada por oscilações entre políticas de autonomia nacional e estratégias de inserção internacional. Esse percurso histórico pode ser dividido em diferentes fases, cada uma com especificidades regulatórias e efeitos distintos sobre o desenvolvimento tecnológico do país.

Com a abertura econômica na década de 1990, a política de reserva de mercado foi encerrada em 1992, o que levou à falência de várias empresas nacionais incapazes de competir com a concorrência estrangeira. Esse período evidencia como a tensão entre o protecionismo industrial e a inovação aberta contribuiu de forma decisiva para o atraso regulatório brasileiro.

A alternância brusca entre um protecionismo rígido e uma liberalização repentina comprometeu a continuidade do desenvolvimento do setor. A falta de uma estratégia de longo prazo, aliada à ausência de políticas públicas estáveis que integrassem indústria, pesquisa e inserção internacional, revelou-se um dos principais entraves ao avanço sustentável da informática no país.

#### 4 NORMAS SOBRE HARDWARE E SOFTWARE

A regulação jurídica referente a *software* e *hardware* no Brasil evoluiu de maneira distinta, refletindo tanto os desafios técnicos e econômicos específicos a cada setor quanto a necessidade de adaptação contínua do ordenamento jurídico a um contexto de inovação tecnológica acelerada.

Cada termo tem uma definição própria. O termo *software* é tecnicamente definido como o conjunto abrangendo o programa de computador, sua descrição e documentação correlata, ou a combinação destes componentes. Barbosa (2018, p. 7) pontua que o cerne da definição normativa de *software* reside precisamente na conjugação do programa de computador e sua documentação técnica associada.<sup>31</sup>

A legislação brasileira, notadamente a Lei nº 7.232, estabeleceu em seu artigo 43 a conceituação de *software* pela agregação do programa de computador à sua documentação técnica associada. Em contraste com o "*hardware*", que constitui um componente físico, o *software* configura o elemento funcional "inteligência" dos sistemas informáticos, fundamental para a viabilização da automação de processos.

Ao caracterizar o *software* como a inteligência dos sistemas, a lei brasileira prefigurou sua posterior proteção híbrida, que reflete sua dupla essência: criativa (como obra intelectual) e funcional (como tecnologia aplicada):

O regime de proteção dos programas de computador segue, em parte, o da Lei 9.610/98, que protege no Brasil os Direitos Autorais. No entanto, com a muitas alterações introduzidas pela Lei 9.609/98, e a natureza claramente tecnológica dos programas de computador, inegavelmente estamos, na Lei em vigor, na presença de um *tertius genus* (Barbosa, 2018, p. 2).

O *hardware*, enquanto objeto de proteção jurídica, abrange criações e inovações no âmbito industrial, garantindo aos seus desenvolvedores direitos exclusivos de uso, fabricação e comercialização. Esses direitos impedem que terceiros explorem tais invenções sem autorização, assegurando a propriedade intelectual sobre modelos de utilidade, desenhos industriais e marcas.

Inicialmente, a ausência de legislação específica para *hardware* no Brasil gerava incertezas quanto ao alcance da proteção e aos mecanismos de defesa dos titulares. A regulamentação desse setor dependia de normas genéricas, como o Código Civil de 1916 e a

---

<sup>31</sup> BARBOSA, Denis Borges. A proteção do software [em linha]. dez. 2018.

Lei de Propriedade Industrial de 1945, que não contemplavam adequadamente as particularidades tecnológicas em rápida evolução (Viegas, 2020, p. 2).

A consolidação de um marco regulatório mais preciso ocorreu apenas em 1996, com a LPI (Lei nº 9.279/1996), que estabeleceu quatro principais formas de proteção, (i) patentes, aplicáveis a invenções inovadoras, como circuitos integrados e dispositivos eletrônicos; (ii) modelos de utilidade, voltados a melhorias funcionais em componentes de computadores; (iii) desenhos industriais, que resguardam o aspecto estético de equipamentos, como *laptops* e *mouses*; (iv) e marcas, que protegem símbolos distintivos associados a produtos de *hardware* (Brasil, 1996).

Além disso, a referida lei regulamentou o segredo industrial, permitindo que empresas mantivessem a confidencialidade de projetos técnicos e processos de fabricação, desde que adotassem medidas adequadas para sua preservação (Brasil, 1996)<sup>32</sup>. Essa inovação foi essencial para setores como o de semicondutores, nos quais a competitividade depende do domínio tecnológico.

A Lei nº 9.279/1996 também previu sanções contra a violação de segredos industriais, estabelecendo que informações confidenciais reveladas em juízo deveriam ser protegidas sob sigilo, vedando seu uso indevido (artigo 206). Além disso, garantiu ao prejudicado o direito de buscar reparação civil (artigo 207) e definiu que a indenização deveria corresponder aos benefícios que teriam sido obtidos sem a violação (artigo 208):

Art. 206. Na hipótese de serem reveladas, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, sejam segredo de indústria ou de comércio, deverá o juiz determinar que o processo prossiga

---

<sup>32</sup> Em relação a algoritmos e *softwares* embarcados, estes são caracterizados como códigos-fonte e arquiteturas de *software* designados para o controle de *hardware*. Tais *softwares* consistem em programas residentes em dispositivos eletrônicos, com a função de controlar suas operações e interagir com o ambiente físico. Uma análise das ferramentas de proteção demonstra que, em situações específicas, a invenção subjacente implementada no *software* embarcado é suscetível de proteção patentária. Este ponto é abordado no Guia Básico de Patente do Instituto Nacional Da Propriedade Industrial (INPI) Rio de Janeiro, 2023. Disponível em: <https://www.gov.br/inpi/pt-br/servicos/patentes/guia-basico-de-patente>. Acesso em: 12 maio 2025 e em publicações da World Intellectual Property Organization (WIPO, *Software and Business Methods*. Geneva: WIPO, 2023. Disponível em: [https://www.wipo.int/patents/en/topics/software\\_business\\_methods.html](https://www.wipo.int/patents/en/topics/software_business_methods.html). Acesso em: 12 maio 2025). A manutenção da confidencialidade do código-fonte e de informações atinentes ao desenvolvimento do *software* embarcado configura, ademais, uma via de proteção alinhada ao segredo industrial. Considera-se, outrossim, a aplicação de Indicação Geográfica (IG) a *hardware*. Um cenário ilustrativo, conforme apresentado no Manual de Indicações Geográficas do Instituto Nacional Da Propriedade Industrial (INPI, Rio de Janeiro, 2021. Disponível em: <https://manualdemarcas.inpi.gov.br/projects/manual-de-indicacoes-geograficas/wiki>. Acesso em: 12 maio 2025), compreende um agrupamento tecnológico que se distingue pela produção de um tipo específico de *hardware*, possuindo características singulares e reconhecimento de qualidade no mercado. Neste contexto, a IG constitui um mecanismo de proteção potencialmente aplicável. Informações contextuais sobre o setor podem ser obtidas em relatórios setoriais, como o Relatório Anual da Indústria Elétrica e Eletrônica da Associação Brasileira Da Indústria Elétrica e Eletrônica (ABINEE), São Paulo, 2023. Disponível em: <https://www.abinee.org.br/>. Acesso em: 12 maio 2025.

em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades. Art. 207. Independentemente da ação criminal, o prejudicado poderá intentar as ações cíveis que considerar cabíveis na forma do Código de Processo Civil. Art. 208. A indenização será determinada pelos benefícios que o prejudicado teria auferido se a violação não tivesse ocorrido (Brasil, 1996).

Posteriormente, a Lei nº 11.484/2007 ampliou a proteção ao incluir a topografia de circuitos integrados, assegurando direitos exclusivos sobre seu *layout*<sup>33</sup> tridimensional e coibindo cópias não autorizadas, conforme se nota a lei em sua redação oficial:

Dispõe sobre os incentivos às indústrias de equipamentos para TV Digital e de componentes eletrônicos semicondutores e sobre a proteção à propriedade intelectual das topografias de circuitos integrados, instituindo o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores - PADIS e o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Equipamentos para a TV Digital – PATVD (Brasil, 2007).

Diante disso, vale destacar que o desafio jurídico está relacionado aos órgãos de registro, uma vez que explicar a natureza do aplicativo nem sempre é uma tarefa simples. O esforço concentra-se na elaboração de novos modelos de contratos que possam estabelecer regras mais claras para todos os envolvidos na cadeia produtiva dos aplicativos (Pinheiro, 2017, p. 222).

Inicialmente, na década de 1970, os *softwares* eram amparados pela Lei nº 5.988/1973<sup>34</sup> (Lei de Direitos Autorais), que os equiparava a obras literárias<sup>35</sup>, embora sem abordar

<sup>33</sup> A topografia de circuitos integrados, também denominada “layout” ou “máscara”, corresponde à configuração tridimensional das camadas de um circuito integrado, como a de um chip, definindo a disposição espacial de seus componentes e interconexões; sua proteção jurídica no Brasil é conferida pela Lei nº 11.484/2007, que alterou dispositivos da Lei nº 9.279/96, distinguindo-se do desenho industrial pela natureza técnica e funcional do objeto protegido, que recai sobre a estrutura do circuito, seu desempenho e funcionalidades. BRASIL. Ministério do Desenvolvimento, Indústria, Comércio e Serviços. INPI. Disponível em: <https://www.gov.br/inpi/pt-br/assuntos/topografias-de-circuitos-integrados/topografia-de-circuitos-integrados-mais-informacoes>. Acesso em: 12 maio 2025).

<sup>34</sup> Antes da promulgação de legislação específica, a proteção jurídica de programas de computador no Brasil era operada por analogia à Lei nº 5.988/73, então vigente sobre direitos autorais, com base na compreensão do software como obra intelectual; nesse contexto, reconheciam-se ao autor direitos morais e patrimoniais, admitia-se o registro no INPI para fins de publicidade e prova, e a aplicação analógica da norma, embora funcional, apresentava limitações quanto à efetividade da tutela (Pinheiro, 2017); em julgamento do TJSP envolvendo uso indevido de software após o fim da licença, a conduta foi tida como ilícita, fixando-se o quantum indenizatório com base no valor das licenças não cedidas, aplicando-se juros de mora e reconhecendo-se sucumbência recíproca nos termos do art. 21 do CPC, com provimento parcial do recurso da ré e desprovimento do recurso da autora. (TJ-SP - AC: 91266766420058260000 SP 9126676-64.2005.8.26.0000, Relator: Fortes Barbosa, Data de Julgamento: 14/12/2011, 8ª Câmara de Direito Privado, Data de Publicação: 16/12/2011). São Paulo. Tribunal de Justiça. Apelação Cível nº 9126676-64.2005.8.26.0000. Relator: Desembargador Fortes Barbosa. São Paulo, 14 dez. 2011. Publicação: 16 dez. 2011. BRASIL. Lei nº 5.988, de 14 de dezembro de 1973. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da União, Brasília, DF, 17 dez. 1973. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l5988.htm](http://www.planalto.gov.br/ccivil_03/leis/l5988.htm). Acesso em: 12 maio 2025.

<sup>35</sup> Para Lessig (1999, p. 136) a regulação via propriedade industrial falhou por não compreender que ‘código é lei’ em ambientes digitais contratos não são tão graves quanto o código, eles fazem parte do direito. Se uma cláusula de contrato contrariar algum princípio do direito autoral, é possível se recusar a cumpri-la e deixar que a outra parte vá à Justiça para tentar fazer valer. Com o código, isso não funciona assim. Os problemas que surgem quando contratos ocupam o lugar do direito autoral ficam ainda piores quando quem ocupa esse lugar é o código. Repito:

especificidades como a proteção do código-fonte ou a possibilidade de patenteamento. A equiparação dos *softwares* a obras literárias decorre do caráter genérico da Lei de Direitos Autorais que, ao regular direitos autorais sem especificar os *softwares*, permitiu seu enquadramento como 'bens móveis' sob a égide de proteção às obras intelectuais:

Art. 1º Esta Lei regula os direitos autorais, entendendo-se sob esta denominação os direitos de autor e direitos que lhe são conexos. Art. 2º Os direitos autorais reputam-se, para os efeitos legais, bens móveis. Art. 3º Interpretam-se restritivamente os negócios jurídicos sobre direitos autorais (Brasil, 1973).

Essa lacuna gerava insegurança jurídica, uma vez que o registro no INPI se limitava à análise formal da documentação, sem avaliar a originalidade técnica do programa, conforme destacado por Pinheiro (2017, p. 127):

(...) o registro de software no INPI possui algumas particularidades, visto que, ao invés de se analisar a originalidade do software em si, o INPI apenas verifica se a documentação formal está correta, sem analisar o seu código-fonte e seus aspectos técnicos. Dessa forma, a concessão de registro de software pelo INPI não significa que o software seja original ou diferente de outros no mercado, mas apenas que o titular fez o pedido de registro de forma correta. Caso o registro seja concedido, o INPI manterá uma cópia lacrada do software em seus arquivos, que somente poderá ser aberta mediante ordem judicial.<sup>36</sup>

A jurisprudência, como no caso julgado abaixo colacionado que reforçou a responsabilização por uso indevido de *softwares*, condicionando indenizações ao valor das licenças violadas, confirmando que a ausência de prevenção eficiente no registro obriga o Judiciário a atuar como reparador após ocorrência do fato:

BRASIL. Tribunal de Justiça. Apelação Cível n.º 9126676-64.2005.8.26.0000. Indenizatória: Uso indevido de programas de computador após o término do prazo de licença ato ilícito caracterizado “Quantum” indenizatório vinculado às licenças que poderiam ser cedidas - Correção quanto à incidência dos juros de mora Sucumbência recíproca Aplicação do art. 21 do CPC Recurso da ré parcialmente provido e recurso da autora desprovido. Relator: Desembargador Fortes Barbosa. São Paulo, 14 dez. 2011. Publicação: 16 dez. 2011.

O setor de Tecnologia da Informação e Comunicação (TIC) no Brasil demonstra notável dinamismo econômico, com o mercado de *software* exibindo crescimento expressivo superior à média global, conforme indicado por dados da ABES e IDC, mesmo em face de cenários

---

como contestar o código? Quando um software impõe sua própria forma de proteção, sem depender do Estado, onde é possível questionar esse tipo de controle? Onde é possível pedir equilíbrio quando o próprio código o elimina? LESSIG, Lawrence. Code and Other Laws of Cyberspace. Nova Iorque: Basic Books, 1999.

<sup>36</sup> PINHEIRO, Patrícia Peck. Direito Digital. 8. ed. São Paulo: Saraiva, 2017.

desafiadores como o pandêmico; a importância do *software* transcende a mera codificação, integrando-se profundamente às atividades econômicas e impulsionando inovações tecnológicas, o que sublinha a criticidade da proteção dos direitos de seus criadores e das Invenções Implementadas por Computador (IIC) (Santos, 2023, p. 6.241).<sup>37</sup>

A evolução contínua da tecnologia transformou programas de computador de criações intangíveis a elementos com aplicação industrial e efeito técnico, potencialmente enquadráveis como invenções patenteáveis sob a LPI, caso atendam aos requisitos legais.<sup>38</sup>

Na economia do conhecimento impulsionada pela inovação complexa e tecnológica, a propriedade intelectual manifesta-se como instrumento estratégico vital para as empresas, fundamental na apropriação de valor, na obtenção de vantagem competitiva e na gestão de ativos intangíveis, com seu arcabouço jurídico e gestão integrada influenciando diretamente as decisões econômicas e a proteção do conhecimento (Romão, 2019, p. 7).<sup>39</sup>

O setor de Tecnologia da Informação e Comunicação (TIC) ganhou relevância econômica, com o mercado de *software* crescendo acima da média global, impulsionado por sua integração em processos produtivos e inovações tecnológicas. A natureza híbrida dos programas (entre criação intelectual e aplicação industrial) levou a debates sobre o regime ideal de proteção.

Enquanto a Lei nº 7.646/1987<sup>40</sup> estabeleceu o registro no INPI como requisito para comprovar autoria:

Art. 1º São livres, no País, a produção e a comercialização de programas de computador, de origem estrangeira ou nacional, assegurada integral proteção aos titulares dos respectivos direitos, nas condições estabelecidas em lei. Parágrafo único. 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,

<sup>37</sup> SANTOS, Givanildo de Jesus, et al. Análise da política brasileira de proteção da propriedade intelectual para *softwares* e invenção implementada por computador (IIC). Observatório de la Economía Latinoamericana, v. 21, n. 7, p. 6239-6262, 2023.

<sup>38</sup> Casella (1986, p. 212) argumenta que “(...) o *software* é, fundamentalmente informação, e como tal só pode ser obra do intelecto”, entretanto, a mesma autora expõe o entendimento diverso à época (1986), qual seja: “A proteção pelo direito de propriedade industrial foi a forma escolhida num primeiro momento, mas a Convenção de Mônaco estabeleceu expressamente no art. 52, que não é considerada invenção protegida pelo direito de propriedade industrial o programa de computador enquanto tal, deixando a possibilidade de invocar esta proteção para os processos produtivos que implicam na utilização de um programa eletrônico”. CASELLA, Adriana Camargo Rodrigues. Proteção do “*software*” pelo direito do de autor. Revista da Faculdade de Direito, Universidade de São Paulo, v. 81, p. 202-221, 1986.

<sup>39</sup> ROMÃO, Carolina Brasil et al. A indústria dos jogos eletrônicos: novas tecnologias, propriedade intelectual e cenário mundial e brasileiro. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 5, n. 1, p. 1-20, 2019.

<sup>40</sup> BRASIL. Lei nº 7.646, de 18 de dezembro de 1987. Dispõe sobre a proteção de propriedade intelectual de programa de computador e sua comercialização no País. Diário Oficial da União, Brasília, DF, 21 dez. 1987. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l7646.htm](http://www.planalto.gov.br/ccivil_03/leis/l7646.htm). Acesso em: 12 maio 2025.



dispositivos, instrumentos ou equipamentos periféricos, baseados em técnica digital, para fazê-los funcionar de modo e para fins determinados (Brasil, 1987).

A Lei nº 9.609/1998<sup>41</sup> consolidou o modelo de direitos autorais, introduzindo avanços como a proteção do código-fonte, a flexibilização do registro (facultativo, mas probatório) e medidas antipirataria:

Proteção do código-fonte: Reconhecido como parte integrante do software. Flexibilidade no registro: O registro no INPI tornou-se facultativo, mas recomendado para fins probatórios. Combate à pirataria: Estabeleceu penalidades mais rigorosas para cópias não autorizadas (Brasil, 1998).

Concomitantemente, a Lei nº 9.610/1998<sup>42</sup> (Lei de Direitos Autorais) complementou o regime, tratando de *softwares* desenvolvidos por empregados e limitando a responsabilidade de provedores.

Para o *hardwares*, a proteção inicialmente é dispersa, baseada no Código Civil de 1916 e na LPI de 1945, foi unificada pela Lei nº 9.279/1996<sup>43</sup>, que permitiu patentes (invenções), modelos de utilidade (melhorias funcionais), desenhos industriais (aspecto estético) e marcas.

A distinção entre *softwares* (protegidos por direitos autorais) e *hardwares* (protegidos por propriedade industrial) tornou-se clara, embora casos de *softwares* embarcados em *hardware* demandem análise específica, como no julgado AREsp 2302494/STJ, que reconheceu a proteção autoral de interfaces gráficas mesmo em dispositivos físicos:

No julgamento do AREsp 230.2494/STJ, reconheceu-se a proteção autoral de softwares mesmo quando embarcados em hardware, aplicando-se a Lei 9.610/98

<sup>41</sup> 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, 20 fev. 1998. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/19609.htm](http://www.planalto.gov.br/ccivil_03/leis/19609.htm). Acesso em: 12 maio 2025.

<sup>42</sup> Tome-se a relação entre as duas normas como normas em relação de aplicação da Lei nº 9610 como norma de aplicação subsidiária à lei geral dos *softwares*. VIEGAS, Cláudia Mara de Almeida Rabelo. Proteção jurídica do *software*. JusBrasil, 2020. Disponível em: <https://www.jusbrasil.com.br/artigos/propriedade-industrialprotecao-juridica-dosoftware/760054078>. Acesso em: 12 maio 2025. Julgado do STJ: Ementa: Apelações Cíveis. Ação inibitória c/c indenização por perdas e danos decorrentes de uso não autorizado de software. Aplicabilidade do regime autoral aos programas de computador, conforme art. 2º da Lei 9.609/98 e Lei 9.610/98. A contrafação configura-se na “reprodução não autorizada” de software (art. 5º, VII, Lei 9.610/98), prática vedada por causar prejuízo ao titular e à sociedade. Laudo pericial comprovou o uso indevido de estrutura funcional de um programa na criação de outro, não justificada por coincidência de ramo de atuação. Indenização fixada nos termos do art. 103, parágrafo único, da Lei 9.610/98: sendo possível quantificar a violação, aplicou-se sanção de 10 vezes o valor de cada software utilizado indevidamente, conforme jurisprudência consolidada do STJ (...). (fl. 1559-1560). (STJ - AREsp: 2302494, Relator: RAUL ARAÚJO, Data de Publicação: 05/09/2023). BRASIL. Superior Tribunal de Justiça. Agravo em Recurso Especial nº 2302494. Relator: Ministro Raul Araújo. Brasília, DF, 5 set. 2023. BRASIL. Lei nº 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/19610.htm](https://www.planalto.gov.br/ccivil_03/leis/19610.htm). Acesso em: 24 maio 2025.

<sup>43</sup> BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Brasília, DF: Presidência da República, 1996.

(Direito Autoral). O Tribunal entendeu que a reprodução não autorizada de programas configura contrafação, independentemente do suporte físico, fixando a indenização em 10 vezes o valor de cada software ilegalmente utilizado, conforme o art. 103 da Lei 9.610/98 (STJ - AREsp: 2302494, Relator: RAUL ARAÚJO, Data de Publicação: 05/09/2023)

A trajetória normativa brasileira na proteção de *software* e *hardware* evidencia um esforço contínuo de adaptação às demandas tecnológicas e econômicas. Observa-se que enquanto o *software* consolidou-se sob o regime de direitos autorais, com avanços como a proteção do código-fonte e medidas antipirataria (Lei nº 9.609/1998), o *hardware* encontrou amparo na LPI (Lei nº 9.279/1996), que viabilizou patentes, modelos de utilidade e a salvaguarda de segredos industriais.

A jurisprudência, como exemplificado pelo AREsp 230.2494/STJ, reforçou a aplicação prática desses regimes, mesmo em casos híbridos de integração entre componentes físicos e lógicos.

A ascensão de tecnologias como IA tensiona as fronteiras entre os regimes de proteção autoral e industrial, exigindo reinterpretações jurídicas e atualizações legislativas. Além disso, a relevância econômica do setor de TIC, com seu crescimento acima da média global (ABES e IDC), sublinha a urgência de um marco legal ágil e coerente, capaz de equilibrar incentivo à inovação, segurança jurídica e competitividade internacional.

A interface entre *hardware* e *software*, como em dispositivos com sistemas embarcados, exige interpretação jurídica cuidadosa. Enquanto o *hardware*<sup>44</sup> é protegido por patentes ou desenhos industriais, *softwares* integrados podem ser tutelados por direitos autorais, gerando sobreposições que demandam harmonização (INPI, 2021). Além disso, a aplicação de Indicação Geográfica (IG) a *hardware*, surge como mecanismo complementar, reconhecendo a qualidade singular de produtos associados a regiões específicas (ABINEE, 2023).<sup>45</sup>

Em síntese a proteção jurídica do *hardware* no Brasil evoluiu de uma fase sem regulamentação para a instauração de marcos legais, como a LPI e a Lei n.º 11.484/2007. Esse progresso consolidou a proteção de invenções e desenhos industriais, alinhando o país a padrões

<sup>44</sup> Com base em análise dos elementos do *hardware* passíveis de proteção, verifica-se que esta abrange aspectos de sua configuração externa. Tais aspectos incluem o formato, compreendendo a configuração espacial tridimensional do objeto, exemplificada na carcaça de um equipamento computacional, no design de um dispositivo de entrada (mouse) ou na conformação de um fone de ouvido. Ademais, incluem-se os ornamentos, definidos como elementos visuais que compõem a estética do produto, tais como texturas, padrões, gravações e detalhes de caráter estético, bem como a combinação de cores, referindo-se à seleção e disposição cromática aplicada ao produto. Instituto Nacional Da Propriedade Industrial (INPI). Manual de Desenho Industrial. Rio de Janeiro: INPI, 2021. Disponível em: <https://manualdemarcas.inpi.gov.br/>. Acesso em: 12 maio 2025. Inovação UNB. O que pode ser protegido pelo desenho industrial. <https://inovacao.uneb.br/o-que-podeser-protetido-pelo-registro-de-desenho-industrial/>. Acesso: 23 maio 2025.

<sup>45</sup> BRASIL. Associação Brasileira da Indústria Elétrica e Eletrônica (ABINEE). Website Institucional. São Paulo: ABINEE, 2023. Disponível em: <https://www.abinee.org.br/>. Acesso em: 12 maio 2025.

internacionais. Contudo, desafios persistem na interface entre *hardware* e *software*, indicando lacunas na harmonização das proteções.

A complexidade contratual e a necessidade de aprimorar registros de aplicativos demandam atualização legislativa. A IG surge como ferramenta complementar, mas sua aplicação ao *hardware* carece de maior desenvolvimento. A efetividade da proteção dependerá de contínuas atualizações legais e da integração entre os agentes envolvidos, visando à manutenção da propriedade intelectual como propulsor de inovação e competitividade.

As novas fronteiras tecnológicas (como os dilemas trazidos pela IA) colocam em tensão o modelo jurídico atual. A IA, em especial, desafia categorias tradicionais ao combinar dimensões lógicas, físicas e industriais, exigindo não apenas revisões conceituais, mas também a criação de novos marcos regulatórios, como propõe o Projeto de Lei nº 21/2020.

## 5 MARCO REGULATÓRIO DIGITAL

A partir da década de 1990, o foco regulatório deslocou-se progressivamente do *hardware* para o *software*, refletindo na revolução digital marcada pela expansão da internet e pelo surgimento de tecnologias disruptivas, como computação em nuvem e inteligência artificial (Cukierman; Castro; Alves, 2012, p. 4).

Inicialmente, a legislação brasileira negligenciou o *software*, dedicando-lhe apenas disposições vagas, enquanto priorizava o *hardware*, uma escolha influenciada pelo potencial comercial imediato da indústria de computadores. Contudo, mesmo durante os debates legislativos, especialistas como Eduardo Guy já alertavam para a relevância estratégica do *software*, considerado mais crucial que o *hardware* a longo prazo:

Observa-se que outro ponto da pauta, o software, foi quase totalmente negligenciado na redação final da lei, provavelmente devido ao fato de que, àquela altura, as apostas no sucesso comercial do hardware (em termos de lucros) ainda serem muito altas. Na verdade, a lei acabou contemplando o software com apenas dois artigos, sendo que um deles apenas afirmava que disposições acerca de software seriam objeto de outras leis mais específicas, a serem aprovadas posteriormente pelo Congresso. Todavia, durante os debates, muitos convidados já alertavam sobre a relevância do software em um futuro próximo. O software já começava a tornar-se valioso, porém dá-se a impressão que o ímpeto e a urgência de legislar sobre a reserva de mercado para a produção de computadores, ou seja, de hardware, aliada à visão de curto prazo dos industriais brasileiros, ‘jogou para escanteio’ a atenção requerida pelo software. A exemplo de muitos dos palestrantes junto à Comissão Mista, Eduardo Guy, da ASSESPRO, durante sua interlocução com os parlamentares, já afirmava que o problema do software era, nas palavras dele, “mais relevante e estratégico” do que o do hardware (Cukierman; Castro; Alves, 2012, p. 4).

Essa negligência inicial em relação ao *software* reflete uma visão de curto prazo que, mais adiante, se mostraria incompatível com as demandas estruturais do governo. A implementação do governo digital exige uma estrutura jurídico-institucional proativa, focada em resultados de longo prazo e na antecipação de demandas sociais via tecnologias. A integração dessas tecnologias deve seguir o princípio "digital por concepção", configurando serviços desde a criação para evitar a mera digitalização da burocracia existente e promover a simplificação administrativa (Carvalho, 2020, p. 129).<sup>46</sup>

Essa necessidade ganha urgência diante dos desafios regulatórios complexos trazidos pela rede. A internet, como rede global descentralizada baseada no protocolo TCP/IP, introduziu

---

<sup>46</sup> CARVALHO, Lucas Borges de. Governo digital e direito administrativo: entre a burocracia, a confiança e a inovação. Revista de Direito Administrativo, [S. l.], v. 279, n. 3, p. 115–148, 2020. Disponível em: <https://periodicos.fgv.br/rda/article/view/82959>. Acesso em: 20 jun. 2025.

desafios regulatórios complexos, demandando equilíbrio entre inovação, direitos fundamentais e segurança (Castells, 2018, p. 478).<sup>47</sup>

No Brasil, a Lei nº 12.965/2014<sup>48</sup> (Marco Civil da Internet) tornou-se o pilar da regulamentação digital, estabelecendo princípios como neutralidade da rede, privacidade dos usuários e liberdade de expressão, para ancorar juridicamente a transformação digital da sociedade.

O MCI também definiu responsabilidades para provedores de conexão e aplicações, limitando a responsabilização destes por conteúdo de terceiros, exceto em caso de descumprimento de ordens judiciais de remoção. Além disso, consagrou o direito ao esquecimento<sup>49</sup>, permitindo a exclusão de dados pessoais obsoletos (Câmara dos Deputados, 2014).

No campo da segurança cibernética, o Decreto nº 10.222/2020<sup>50</sup> instituiu a Estratégia Nacional de Segurança Cibernética (E-Ciber), priorizando a proteção de infraestruturas críticas (como energia e saúde) e a conscientização pública sobre riscos digitais.

A resposta normativa brasileira à criminalidade digital materializou-se, notadamente, primeiro com a promulgação da Lei nº 12.735/2012<sup>51</sup> (Lei Azeredo) e depois com a Lei nº 12.737/2012<sup>52</sup> (Lei Carolina Dieckmann).

<sup>47</sup> CASTELLS, Manuel. A sociedade em rede. 19. ed. São Paulo: Paz e Terra, 2018.

<sup>48</sup> BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 6 de abr. de 2025.

<sup>49</sup> O STF negou o direito ao esquecimento como garantia fundamental no RE nº 1.010.606/RJ, priorizando abstratamente a liberdade de expressão sobre direitos à privacidade e honra. Contudo, falhou ao não estabelecer critérios concretos para sopesar esses direitos em casos específicos, gerando insegurança jurídica sobre como resolver colisões entre liberdade informativa e proteção da personalidade na prática. (RE 1010606, Relator(a): DIAS TOFFOLI, Tribunal Pleno, julgado em 02-11-2021, Processo Eletrônico Repercussão Geral - Mérito DJe-096 Divulg 19-05-2021 Público 20-05-2021). BRASIL. STF. Recurso Extraordinário nº 1.010.606/RJ. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur446557/false>. Acesso em 20 jun. 2025. DEOCLECIANO, Pedro Rafael Malveira; LOBO, Julio César Matias; VIANA, Janile Lima. Uma análise crítica da atual posição do Supremo Tribunal Federal sobre o direito ao esquecimento. Revista Brasileira de Direito Civil, v. 31, n. 02, p. 203-203, 2022.

<sup>50</sup> BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/decreto/d10222.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm). Acesso em: 6 de abr. de 2025.

<sup>51</sup> BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12735.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm). Acesso em: 30 maio 2025.

<sup>52</sup> BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm). Acesso em: 6 de abr. de 2025.

A Lei n.º 12.735/2012 incorporou ao ordenamento jurídico disposições para o enfrentamento de crimes cibernéticos, ajustando procedimentos e aprimorando mecanismos de investigação e persecução de delitos informáticos.

Em simultâneo, a Lei Carolina Dieckmann tipificou crimes cibernéticos, como invasão de dispositivos e divulgação não autorizada de dados, alinhando o Brasil a padrões internacionais de combate ao cibercrime (Brasil, 2012). Essa lei prevê penas que variam de detenção a reclusão, dependendo da gravidade da conduta, como o acesso não autorizado a comunicações particulares ou segredos industriais:

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de um sexto a um terço se a invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave (Brasil, 2012).

No âmbito dos jogos eletrônicos, o marco legal, Lei nº 14.852/2024<sup>53</sup>, buscou fomentar a indústria nacional por meio de incentivos fiscais e classificação etária transparente, além de proteger crianças contra microtransações abusivas. Tal legislação distingue claramente jogos de entretenimento de apostas eletrônicas, estas sujeitas a regras mais rígidas, como a exigência de licenças estatais previstas na Lei nº 13.756/2018.<sup>54</sup>

Apesar dos avanços na regulação de nichos como jogos eletrônicos a regulação do poder econômico das plataformas digitais (como marketplaces e redes sociais) ainda é incipiente.

<sup>53</sup> BRASIL. Lei nº 14.852, de 3 de maio de 2024. Cria o marco legal para a indústria de jogos eletrônicos; e altera as Leis nºs 8.313, de 23 de dezembro de 1991, 8.685, de 20 de julho de 1993, e 9.279, de 14 de maio de 1996. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2024/lei/114852.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/114852.htm). Acesso em: 6 de abr. de 2025.

<sup>54</sup> BRASIL. Lei nº 13.756, de 12 de dezembro de 2018. Dispõe sobre o Fundo Nacional de Segurança Pública (FNSP), sobre a destinação do produto da arrecadação das loterias e sobre a promoção comercial e a modalidade lotérica denominada apostas de quota fixa; altera as Leis nº 8.212, de 24 de julho de 1991, 9.615, de 24 março de 1998, 10.891, de 9 de julho de 2004, 11.473, de 10 de maio de 2007, e 13.675, de 11 de junho de 2018; e revoga dispositivos das Leis nº 6.168, de 9 de dezembro de 1974, 6.717, de 12 de novembro de 1979, 8.313, de 23 de dezembro de 1991, 9.649, de 27 de maio de 1998, 10.260, de 12 de julho de 2001, 11.345, de 14 de setembro de 2006, e 13.155, de 4 de agosto de 2015, da Lei Complementar nº 79, de 7 de janeiro de 1994, e dos Decretos-Leis nº 204, de 27 de fevereiro de 1967, e 594, de 27 de maio de 1969, as Leis nº 6.905, de 11 de maio de 1981, 9.092, de 12 de setembro de 1995, 9.999, de 30 de agosto de 2000, 10.201, de 14 de fevereiro de 2001, e 10.746, de 10 de outubro de 2003, e os Decretos-Leis nº 1.405, de 20 de junho de 1975, e 1.923, de 20 de janeiro de 1982. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113756.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113756.htm). Acesso em: 6 de abr. de 2025.

Embora a Lei nº 12.529/2011<sup>55</sup> (Lei de Defesa da Concorrência) seja aplicável, lacunas persistem no tratamento de práticas anticompetitivas, como o uso abusivo de dados e a formação de ecossistemas fechados. Propostas em discussão sugerem normas específicas para plataformas com relevância sistêmica (Brasil, 2011).

O exame do enquadramento jurídico das plataformas digitais no sistema normativo brasileiro indica sua sujeição tanto às disposições de direito privado relativas à concorrência desleal quanto às regras de direito econômico, especificamente a Lei nº 12.529/2011, evidenciando a necessidade de adaptação normativa à complexidade digital.

Não obstante, um exame empreendida pela Secretaria de Reformas Econômicas do Ministério da Fazenda, consoante estudo recentemente divulgado, aponta para a identificação de lacunas no arcabouço regulatório vigente em face das particularidades inerentes aos ambientes digitais (Brasil, 2024).<sup>56</sup>

Tais especificidades abrangem fenômenos como os efeitos de rede, caracterizados pelo incremento do valor da plataforma em função do aumento da base de usuários; a configuração de mercados multilaterais, que articulam múltiplos grupos de agentes econômicos em interações de benefício recíproco; a expressiva coleta e processamento de dados, empregados na personalização de serviços e estratégias de publicidade; e a formação de ecossistemas complexos, compostos por interconexão de empresas e serviços (Brasil, 2024).

A investigação, que se dedicou à exploração dos aspectos econômicos e concorrenciais destas plataformas no território nacional, evidencia desafios regulatórios primordiais, incluindo a aferição de poder de mercado, o controle de atos de concentração econômica e a necessidade de mecanismos preventivos mais eficazes. Como proposição para a superação destes desafios, o estudo sugere a implementação de tratamento regulatório específico, contemplando a definição de critérios para determinação de relevância sistêmica das plataformas (Brasil, 2024).<sup>57</sup>

---

<sup>55</sup> BRASIL. Lei nº 12.529, de 30 de novembro de 2011. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica; altera a Lei no 8.137, de 27 de dezembro de 1990, o Decreto-Lei no 3.689, de 3 de outubro de 1941 - Código de Processo Penal, e a Lei no 7.347, de 24 de julho de 1985; revoga dispositivos da Lei no 8.884, de 11 de junho de 1994, e a Lei no 9.781, de 19 de janeiro de 1999; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12529.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12529.htm). Acesso em: 6 de abr. de 2025.

<sup>56</sup> BRASIL. Ministério da Fazenda. Secretaria de Reformas Econômicas. Plataformas Digitais: Aspectos Econômicos e Concorrenciais e Recomendações para Aprimoramentos Regulatórios no Brasil. Brasília, DF: Ministério da Fazenda, 2024.

<sup>57</sup> POLIDO, Fabrício; ANJOS, Lucas (orgs.). Marco Civil e Governança da Internet: diálogos entre o doméstico e o global. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2016. BRASIL. Ministério da Fazenda. Secretaria de Reformas Econômicas. Plataformas Digitais: Aspectos Econômicos e Concorrenciais e Recomendações para Aprimoramentos Regulatórios no Brasil. Brasília, DF: Ministério da Fazenda, 2024.

Esta abordagem preconiza a manutenção da aplicação da legislação antitruste tradicional, concomitantemente à introdução de adaptações normativas ou à criação de regulamentação específica, visando a acomodar a dinâmica particular dos ecossistemas digitais e sua crescente projeção na estrutura econômica.

Desde a priorização do *hardware* nos anos 90, passando pelo MCI até a legislação de jogos eletrônicos, o Brasil demonstrou adaptabilidade às demandas digitais. Os marcos legais buscaram alinhar o país a padrões internacionais, assegurando direitos fundamentais e combatendo a criminalidade digital. Contudo, lacunas regulatórias persistem, especialmente quanto ao poder econômico das plataformas digitais.

Fenômenos como efeitos de rede e a coleta massiva de dados exigem respostas normativas ágeis. Os estudos recentes indicam a necessidade de critérios para identificar plataformas de relevância sistêmica e adaptar a legislação antitruste aos ecossistemas digitais.

## 5.1 Internet

A gestão institucional da internet no Brasil consolidou-se progressivamente, antecedendo até mesmo o MCI. Um dos primeiros alicerces foi a Medida Provisória nº 2.200-2/2001<sup>58</sup>, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil). Essa iniciativa estabeleceu certificados digitais para validar transações eletrônicas, impulsionando o comércio digital e a modernização de serviços públicos, como declarações fiscais online (Brasil, 2020).

---

<sup>58</sup> A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) constitui um conjunto de técnicas e procedimentos estabelecidos com o objetivo de assegurar a autenticidade, a integridade e a validade jurídica de documentos em formato eletrônico, fundamentando sua operação na utilização de certificados digitais para a identificação de indivíduos e entidades no ambiente da internet. No contexto desta infraestrutura, a assinatura digital representa uma manifestação eletrônica baseada em criptografia assimétrica, que emprega um par de chaves criptográficas (uma privada e uma pública) para sua geração e verificação. Em um escopo mais amplo, a assinatura eletrônica é definida como qualquer método em meio eletrônico utilizado para identificar o signatário de um documento e para expressar sua concordância com o conteúdo ou intenção vinculada a ele. A disciplina legal da assinatura eletrônica no Brasil é regulamentada pela Lei nº 14.063, de 23 de setembro de 2020, que não apenas a define, mas também estabelece sua classificação em três níveis: a assinatura simples, correspondente a qualquer método eletrônico que permita a identificação do signatário; a assinatura avançada, que se caracteriza por oferecer um grau superior de segurança, mediante a utilização de dados biométricos ou dispositivos portáteis de autenticação (tokens); e a assinatura qualificada, que equivale legalmente à assinatura digital tradicional, sendo baseada em certificado digital emitido por uma Autoridade Certificadora credenciada no âmbito da ICP-Brasil. BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Instituto Nacional de Tecnologia da Informação. ICP-Brasil. Disponível em: <https://www.gov.br/iti/pt-br/assuntos/icp-brasil>. Acesso em: 29 jun. 2025.



Complementarmente, a Lei nº 10.973/2004<sup>59</sup> (Lei de Inovação Tecnológica) fomentou pesquisas em segurança de redes e protocolos de comunicação, ao definir incentivos para instituições científicas e tecnológicas (BRASIL, 2004). O artigo 2º da lei introduziu conceitos-chave, como agências de fomento (instituições financiadoras), ICTs (órgãos públicos de pesquisa) e inovação (desenvolvimento de novos produtos/serviços), estruturando o ecossistema de inovação nacional.

A Lei nº 12.737/2012<sup>60</sup> representou um avanço ao tipificar delitos como invasão de dispositivos e divulgação não autorizada de dados, respondendo a casos emblemáticos de exposição indevida de informações.

Posteriormente, surgiu o Decreto nº 7.962/2013<sup>61</sup>, que regulamenta a Lei nº 8.078, de 11 de setembro de 1990 CDC, com o objetivo de dispor sobre a contratação no comércio eletrônico. Essa regulamentação configura um marco regulatório fundamental para as relações de consumo no ambiente digital no Brasil.

Destaca-se que ao detalhar as obrigações dos fornecedores em termos de informação, atendimento e respeito ao direito de arrependimento, o Decreto visa fortalecer a proteção do consumidor no comércio eletrônico, conferindo maior segurança e transparência a este tipo de transação (Brasil, 2013).

Observa-se que a jurisprudência brasileira tem consolidado a responsabilidade objetiva de provedores por falhas de segurança. O Tribunal de Justiça do Distrito Federal, por exemplo, manteve a sentença que condenou a Facebook a restabelecer o acesso do usuário à conta e pagar indenização por danos morais, entendendo que a responsabilidade da empresa é objetiva, baseada no risco da atividade, e que a falha de segurança permitiu a invasão por terceiros (Brasil, TJDF, 2023).

Nessa decisão, também mencionaram a teoria do fortuito interno, onde a ação de terceiros não quebra o nexo causal, mantendo a responsabilidade da empresa: “A responsabilidade civil dos fornecedores de serviços, a cujo conceito se amolda a ré, é objetiva,

---

<sup>59</sup> BRASIL. Lei nº 10.973, de 2 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2004-2006/2004/lei/110.973.htm](https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/110.973.htm). Acesso em: 6 de abr. de 2025.

<sup>60</sup> BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/112737.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm). Acesso em: 24 maio 2025.

<sup>61</sup> A norma demonstra a preocupação em adaptar os princípios do Código de Defesa do Consumidor à dinâmica específica das compras online, buscando equilibrar os interesses das partes envolvidas e coibir práticas que possam configurar lesão aos direitos consumeristas no ambiente virtual. BRASIL. Decreto nº 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/decreto/d7962.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm). Acesso em: 18 maio 2025.

fundada no risco da atividade desenvolvida, conforme artigos 14 do CDC e 186, 187 e 927 do CC, não se fazendo necessário perquirir acerca da existência de culpa”.<sup>62</sup>

Colaciona-se outro exemplo ilustrativo que ocorreu no Tribunal de Justiça de São Paulo, que a autora teve sua conta invadida e não conseguiu recuperá-la. A sentença inicial considerou improcedente o pedido, mas o TJSP deu provimento parcial ao recurso, reconhecendo o dano moral e condenando a *Facebook* ao pagamento indenizatório, no entanto, não obrigou a reativação da conta por entender que era inviável devido ao cancelamento definitivo. O TJSP também aplicou a responsabilidade objetiva, mas divergiu na quantia indenizatória e na possibilidade de restabelecimento da conta, como se observa no seguinte trecho da decisão:

O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar. [...] o simples fato de que houve o ingresso da conta por terceiro não autorizado, é suficiente para permitir a conclusão de que aconteceu sofrimento pessoal bastante para autorizar a responsabilização da ré pelo pagamento de indenização por danos morais. Tribunal de Justiça. 20ª Câmara de Direito Privado. (Apelação Cível nº 1017172-48.2022.8.26.0007. Relator: Desembargador Luís Carlos de Barros. Diário da Justiça Eletrônico, São Paulo, 13 fev. 2025).<sup>63</sup>

Os litígios no âmbito judicial evidenciam a importância do arcabouço normativo criado; enquanto o MCI estabeleceu bases como neutralidade da rede, privacidade com consentimento e responsabilidade gradativa de provedores, a LGPD detalhou padrões técnicos para prevenção de violações como a do caso em tela.

O MCI, promulgado em 2014, estabeleceu três princípios fundamentais: (i) Neutralidade da rede: Vedação à discriminação no tráfego de dados; (ii) Proteção à privacidade: Exigência de consentimento explícito para coleta de dados pessoais e; (iii) Responsabilidade de provedores: Limitação da responsabilização por conteúdos de terceiros, exceto por descumprimento de ordens judiciais de remoção.

O Marco Civil também introduziu o direito ao esquecimento, permitindo a exclusão de dados desatualizados, embora sujeito a controvérsias sobre seu impacto na liberdade de informação (STF, 2024). Em 2020, o Decreto nº 10.278<sup>64</sup> regulamentou a LGPD, exigindo

<sup>62</sup> BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. Acórdão n. 1719828. Apelação Cível n. 0702233-67.2022.8.07.0007. Relator: Desembargador Alfeu Machado, 6ª Turma Cível, Data de Julgamento: 29 jun. 2023, Data de Publicação: 29 jun. 2023. Disponível em: <https://pje2i.tjdft.jus.br/consultap>. Acesso em: 21 maio 2025.

<sup>63</sup> Para mais informações pesquisa: BRASIL. Tribunal de Justiça. 20ª Câmara de Direito Privado. Apelação Cível nº 1017172-48.2022.8.26.0007. Relator: Desembargador Luís Carlos de Barros. Diário da Justiça Eletrônico, São Paulo, 13 fev. 2025. Disponível em: <https://esaj.tjsp.jus.br/pastadigital/sg/abrirConferenciaDocumento.do>. Acesso em: 21 maio 2025.

<sup>64</sup> BRASIL. Decreto nº 10.278, de 18 de março de 2020. Regulamenta o disposto no inciso X do caput do art. 3º da Lei nº 13.874, de 20 de setembro de 2019, e no art. 2º-A da Lei nº 12.682, de 9 de julho de 2012, para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos

padrões técnicos como criptografia e gestão segura de metadados, reforçando a proteção de dados em um cenário de crescentes ataques *ransomware* (Brasil, 2020).

Por si só a regulação digital não é suficiente para resolução de casos no judiciário, também é necessário harmonização com garantias constitucionais, como demonstra o julgado do STF (Rcl 62174 MG, 2024). Ao anular ordem de remoção total de conteúdo crítico a um profissional, o tribunal reafirmou que os excessos na liberdade de expressão devem ser reparados por direito de resposta ou indenização, não por censura prévia, alinhando-se ao entendimento da ADPF 130 e limitando até mesmo as hipóteses de remoção previstas no MCI:

Direito civil e constitucional. liberdade de expressão e de informação jornalística. Decisão que determina a total retirada de conteúdo. em canais na internet sob pena de multa diária. Alegação de violação à ADPF 130 (...) Inobservância da proporcionalidade e da razoabilidade. excessos devem ser alvo de reparação mediante retificação, direito de resposta ou indenização. i. Caso em exame 1. Cuida-se de reclamação constitucional ajuizada em face de decisão judicial que determinou que jornalista retirasse de seus canais na internet publicações que continham opiniões negativas sobre a atuação de outro profissional, bem como não promovesse nova veiculação. II. Questão em discussão 2. A questão em discussão consiste em saber se viola a liberdade de expressão e de informação jornalística, conforme assentado na ADPF 130, decisão judicial que, sob pena de multa diária, determina a retirada e veda nova veiculação de publicações contendo opiniões negativas sobre a atuação profissional de outrem. III. Razões de decidir 3. É cabível a reclamação cujo paradigma seja a ADPF 130 nos casos que versam sobre conflitos entre liberdade de expressão e informação e a tutela de garantias individuais como os direitos da personalidade (Precedentes: Rcl 22328, Rcl 25.075 e Rcl 28747 AgR). 4. No julgamento da ADPF 130, esta Corte assentou que é excepcional qualquer tipo de intervenção estatal na divulgação de notícias e de opiniões, na medida em que a liberdade de expressão é pré-condição para o exercício esclarecido dos demais direitos e liberdades. Por essa razão, o uso abusivo da liberdade de expressão deve ser reparado, preferencialmente, por meio de retificação, direito de resposta ou indenização. 5. O acórdão reclamado expressamente confirmou a necessidade de retirada total de conteúdo supostamente ofensivo à credibilidade profissional de outrem, bem como vedou novas veiculações, o que efetivamente viola os parâmetros estabelecidos na ADPF 130 (reparação, indenização e direito de resposta). 6. O eventual excesso no exercício da liberdade de informar e na manifestação de opiniões por parte de jornalistas, ainda que o conteúdo esteja relacionado à experiência particular do profissional, não autoriza, como regra geral, a total retirada do conteúdo publicado ou total vedação à publicação. IV. Dispositivo 7. Reclamação constitucional julgada procedente. (STF - Rcl: 62174 MG, Relator: Min. Flávio Dino, Data de Julgamento: 21/10/2024, Primeira Turma, Data de Publicação: Processo Eletrônico DJe-s/n DIVULG 24-10-2024 PUBLIC 25- 10-2024)

A evolução normativa demonstra um esforço contínuo para equilibrar inovação, segurança e direitos fundamentais. Enquanto o MCI e a LGPD representam marcos legais robustos, desafios persistem na aplicação prática, especialmente em casos de conflito entre transparência, liberdade de expressão e responsabilização de agentes digitais.

Apesar disso, a legislação enfrenta desafios em casos em que ilícitos transcendem o ambiente online, como ataques de *ransomware*<sup>65</sup> e fraudes financeiras via PIX, que demandam interpretação sistêmica do CDC para responsabilizar instituições por falhas operacionais.

Nesse sentido, a jurisprudência tem reconhecido que, tratando-se de relação de consumo, a responsabilidade do prestador de serviço independe de culpa. Como ilustra recente decisão do TJ-MS, empresas devem adotar mecanismos eficazes de controle e prevenção de danos. Diante da falha na prestação do serviço bancário, foi determinada a restituição dos valores transferidos via PIX a contas fraudulentas, considerando a negligência da instituição financeira no processo de abertura dessas contas:

Tratando-se de relação regida pelo Código de Defesa do Consumidor, o réu apelante responde, independentemente de culpa, pelos danos causados ao consumidor em razão dos defeitos em seus serviços, de modo que a preliminar de ilegitimidade deve ser rejeitada. As empresas prestadoras de serviços, tal como a apelante, devem possuir mecanismos eficazes de controle de qualidade dos produtos e serviços ofertados, especialmente em relação à política de prevenção de danos, sob pena de responsabilização (art. 14, do CDC). Considerando a falha na prestação de serviço do réu, cabível a condenação à restituição dos valores transferidos pelo consumidor, via PIX, para contas abertas pelos terceiros fraudadores de forma irregular junto à instituição financeira. (TJ-MS - Apelação Cível: 0826377- 93.2022.8.12.0001 Campo Grande, Relator: Juiz Alexandre Branco Pucci, Data de Julgamento: 09/05/2024, 3ª Câmara Cível, Data de Publicação: 10/05/2024) (Brasil, 2024).<sup>66</sup>

Além das questões consumeristas, a responsabilidade civil no ambiente digital também se estende às plataformas *online*, especialmente diante de conteúdos ofensivos publicados por terceiros. Decisões como o ARE 660.861/STF (2012), por exemplo, revelam os tensionamentos entre liberdade de expressão e os direitos da personalidade, como honra e imagem. O Supremo Tribunal Federal (STF) tem enfatizado que a remoção de conteúdo deve observar a proporcionalidade, evitando censura prévia, mas também assegurando reparação às vítimas:

Google – Redes Sociais – Sites de Relacionamento – Publicação de Mensagens na Internet – Conteúdo Ofensivo – Responsabilidade Civil do Provedor – Danos Morais – Indenização – Colisão Entre Liberdade de Expressão E De Informação vs. Direito

<sup>65</sup> O'kane, Sezer e Carlin (2018) analisam as táticas do *ransomware*, que visa bloquear o acesso da vítima ao sistema ou aos dados, condicionando sua liberação ao pagamento de resgate; o software malicioso instrui sobre os procedimentos para desbloqueio e, em versões iniciais, fazia uso de intimidação psicológica, simulando ações policiais e, em casos extremos, exibindo conteúdos ilegais como pornografia infantil, com ameaças de exposição pública e consequências judiciais, estratégias que, em situações dramáticas, culminaram até mesmo em suicídios. O'KANE, Philip; SEZER, Sakir; CARLIN, Domhnall. *Evolução do ransomware*. Iet Networks, v. 7, n. 5, p. 321-327, 2018.

<sup>66</sup> BRASIL. Terceira Câmara Cível do Tribunal de Justiça do Mato Grosso do Sul. Apelação Cível nº 0826377-93.2022.8.12.0001, Apelação em Ação de Rescisão Contratual e Indenização Por Dano Moral e Material. Relator: Juiz Alexandre Branco Pucci. Campo Grande, MS, 09 de maio de 2024. Campo Grande, 10 maio de 2024. Disponível em: <https://esaj.tjms.jus.br/cjsg/getArquivo.do?cdAcordao=1555281&cdForo=0>. Acesso em: 22 jun. 2025.

À Privacidade, À Intimidade, À Honra e À Imagem. Repercussão Geral Reconhecida Pelo Plenário Virtual Desta Corte. (STF - ARE: 660861 MG 9002893-47.2010.8.13.0024, Relator: Luiz Fux, Data de Julgamento: 22/03/2012, Tribunal Pleno, Data de Publicação: 07/11/2012).<sup>67</sup>

Desde a criação da ICP-Brasil (2001) e a instauração do MCI e da LGPD, o Brasil tem demonstrado esforço em harmonizar inovação, segurança e direitos fundamentais. A legislação e a jurisprudência consolidaram a proteção contra crimes cibernéticos e consumeristas, atribuindo responsabilidade objetiva a provedores por falhas de segurança.

O STF, por sua vez, estabelece limites para conflitos entre liberdade de expressão e direitos da personalidade. No entanto, o aumento de ataques como *ransomware*, fraudes via PIX e a complexidade do direito ao esquecimento revelam desafios. Superá-los exige não apenas evolução normativa, mas uma hermenêutica jurídica capaz de integrar os princípios constitucionais, consumeristas e digitais de forma coesa e eficaz.

## 5.2 Proteção de Dados

Os dados pessoais se consolidaram como recurso econômico central da era atual, impulsionando a economia orientada por dados e exercendo influência profunda nas dimensões sociopolítica e individual. Segundo Frazão, Oliva e Tepedino (2020, p. 22) “(...) os dados pessoais como os principais recursos econômicos da nossa época, revela importante ponto de partida para a compreensão da necessidade de proteção dos dados pessoais”. Nesse contexto, os dados pessoais da pessoa natural tornaram-se elementos indispensáveis para o funcionamento de diversas relações comerciais:

(...) no mundo em que se vive atualmente, os dados pessoais da pessoa natural são necessários e até essenciais para diversas áreas comerciais, como, por exemplo, declaração de imposto de renda retido na fonte, na relação de trabalho, no contrato de trabalho, na relação com plano de saúde, que se fazem necessários, além dos dados pessoais comuns, de dados pessoais sensíveis, como tipo sanguíneo, conhecimento de doenças pré-existentes, convicção religiosa etc. (Santos; Carvalho, 2020, p. 20).<sup>68</sup>

Portanto, a exponencialização da capacidade de análise de dados por tecnologias avançadas amplificou o poder associado a seu uso, tornando crítica sua regulamentação como

<sup>67</sup> BRASIL. Supremo Tribunal Federal. Recurso Extraordinário Com Agravo nº 660861. Relator: Ministro Luiz Fux. Brasília, DF, 22 de março de 2012. Brasília, 07 nov. 2012. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4155926>. Acesso em: 02 maio 2025.

<sup>68</sup> SANTOS, Regiane Martins dos; CARVALHO, Adriana Cristina França Leite de. Comentários à Lei Geral de Proteção de Dados. São Paulo: OAB, 2020.

desafio político contemporâneo essencial à harmonização entre avanço tecnológico e a tutela de direitos:

Vistos já como o novo petróleo, os dados são hoje insumos essenciais para praticamente todas as atividades econômicas e se tornaram, eles próprios, objeto de crescente e pujante mercado. Não é sem razão que se cunhou a expressão *data-driven economy*, ou seja, economia movida a dados, para designar o fato de que, como aponta Nick Srnicek, o capitalismo do século XXI passou a centrar-se na extração e no uso de dados pessoais (Frazão; Oliva; Tepedino, 2020, p. 22).

O arcabouço normativo brasileiro para proteção de dados pessoais desenvolveu-se progressivamente, acompanhando as transformações tecnológicas e as demandas sociais por privacidade. Apesar dos avanços normativos, evidencia-se dificuldades de adaptação à nova legislação no contexto brasileiro.<sup>69</sup>

A Constituição Federal de 1988 já consagrava em seu artigo 5º a inviolabilidade da intimidade e da vida privada, estabelecendo as bases para a proteção de informações pessoais. Contudo, foi o CDC (1990) que introduziu as primeiras disposições específicas, garantindo aos cidadãos o direito de acesso e retificação de dados em cadastros comerciais.

Um marco significativo ocorreu em 1997 com a Lei nº 9.507/1997<sup>70</sup>, que regulamenta do *habeas data*, que assegurou o acesso a registros mantidos por entidades governamentais ou de caráter público. Embora importante, este instrumento mostrava-se limitado por restringir-se principalmente às relações entre cidadãos e o Estado, não abarcando adequadamente as complexidades do ambiente digital que se avizinhava<sup>71</sup>:

<sup>69</sup> Para Gualda (2019) “O Brasil não detém uma cultura de proteção de dados pessoais e isso repercute nas práticas corporativas. Continua corriqueira a existência de bases de clientes em planilhas sem controle de acesso, trocas de e-mails com essas bases, uso de dados pessoais de clientes para fins distintos do propósito da coleta, manutenção de dados pessoais por períodos indefinidos e sem controle de segurança, atividades de marketing não regulares, etc. As organizações devem investir em revisitar cada uma de suas linhas de negócio e práticas a elas inerentes, além de treinamento contínuo para colaboradores. A grande maioria dos problemas de violação de dados pessoais e segurança da informação têm por causa condutas inadequadas e a mudança de cultura corporativa é muito mais lenta e muito mais difícil que a troca ou implantação de um *software*. Não devemos subestimar a importância e o desafio cultural que a LGPD traz consigo.” GUALDA, Diego de Lima. Desafio Cultural da Proteção de Dados [acesso eletrônico]. Disponível em: <https://aarb.org.br/desafio-cultural-da-protecao-de-dados/>. Acesso em 14 maio 2025.

<sup>70</sup> “Observe-se que a Lei nº 9.507 ampliou em certa medida o âmbito do remédio previsto no art. 5º nº LXXII, da Constituição da República. (...) O legislador ordinário aditou uma terceira possibilidade: a da anotação, nos assentamentos da entidade ou órgão, da ‘contestação ou explicação’ do interessado. (...) Sublinhe-se que anotar contestação ou explicação não é o mesmo que retificar dado constante do banco ou registro: na retificação, modifica-se (...); na anotação, acrescenta-se algo ao que consta do banco ou registro” (Moreira, 1998, p. 63). MOREIRA, José Carlos Barbosa. O *habeas data* brasileiro e sua lei regulamentadora. Revista de Direito Administrativo, v. 211, 1998. BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/19507.htm](https://www.planalto.gov.br/ccivil_03/leis/19507.htm). Acesso em: 29 jun. 2025.

<sup>71</sup> De acordo com Dallari, a Lei 9.507, ao exigir a prova da recusa, “consagrou a via mais difícil para os interessados, pois a prova da recusa só poderá ser feita se for tentada previamente a via administrativa, o que poderá significar embaraços e retardamento, além de ser de duvidosa constitucionalidade essa exigência posta por

Art. 7º Conceder-se-á habeas data: I - para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; II - para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo; III - para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro, mas justificável e que esteja sob pendência judicial ou amigável (Brasil, 1997).

A Lei n.º 12.527/2011<sup>72</sup> (Lei de Acesso à Informação) representou outro avanço ao estabelecer princípios de transparência na administração pública, incluindo a obrigatoriedade de tratamento responsável de dados pessoais:

Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes: I - observância da publicidade como preceito geral e do sigilo como exceção; II - divulgação de informações de interesse público, independentemente de solicitações; III - utilização de meios de comunicação viabilizados pela tecnologia da informação; IV - fomento ao desenvolvimento da cultura de transparência na administração pública; V - desenvolvimento do controle social da administração pública (Brasil, 2011).

Paralelamente, o MCI (2014) introduziu conceitos fundamentais como o consentimento para coleta de dados e a neutralidade da rede, preparando o terreno para a posterior edição da LGPD<sup>73</sup> em 2018. A lei mais recente trouxe atualizações e especificações para a lei anterior, especialmente no que tange à exclusão de dados pessoais.<sup>74</sup>

---

lei ordinária.” DALLARI, Dalmo de Abreu. O habeas data no sistema jurídico brasileiro. Revista da Faculdade de Direito, Universidade de São Paulo, v. 97, p. 239-253, 2002.

<sup>72</sup> A Lei de Acesso à Informação (LAI) fundamenta-se no princípio da publicidade como regra e do sigilo como exceção, partindo da premissa de que a informação pública é patrimônio do cidadão, impondo ao Estado deveres de transparência; assegura-se a qualquer pessoa, física ou jurídica, o direito de acesso à informação, cabendo aos órgãos públicos o fornecimento dos dados solicitados, bem como a divulgação proativa de conteúdos de interesse coletivo e a preservação da integridade das informações sob sua guarda. BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/l12527.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm). Acesso em 12 maio 2025.

<sup>73</sup> Segundo Frazão, Oliva e Tepedino, “no Brasil, muito embora já houvesse disciplina sobre a proteção de dados, conforme tratado em tópico anterior, sua setorização e pulverização em leis e decretos esparsos, por certo, obstaculiza a visualização de um sistema. A edição da Lei 13.709/2018, significa, nesse contexto, uma orientação para organização formal desse sistema, a partir da cristalização e reprodução de muitos desses dispositivos esparsos, inclusive com status principiológico em alguns casos.” FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. Thomson Reuters Brasil, 2020.

<sup>74</sup> Analisando a relação normativa entre a LGPD e o MCI, observa-se que as inovações conceituais e procedimentais introduzidas pela LGPD impõem a necessidade de atualização do MCI. Especificamente, verifica-se a vedação, imposta aos provedores de aplicações de internet, da guarda de dados pessoais que excedam a finalidade para a qual foi obtido o consentimento do titular, ressalvadas as exceções previstas na própria LGPD.

Para Franco (2024, p. 69), sinteticamente, o MCI estabeleceu bases pioneiras para a governança digital no Brasil, classificando redes sociais como provedoras de aplicações e priorizando a prevenção à censura através do artigo 19<sup>75</sup>, que limita a remoção de conteúdo a ordens judiciais.

Para o autor, essa abordagem binária (remover/não remover) concedeu ampla liberdade às plataformas para autorregulação via termos de uso, mas mostra-se insuficiente ante as complexidades atuais da moderação de conteúdo. Segundo análise do autor supracitado, críticos apontam que o MCI negligencia formas intermediárias de moderação e defendem uma interpretação sistêmica que integre o Código Civil, CDC e LGPD para abordagens mais refinadas (Franco, 2024, p. 69).

Já a LGPD estabelece transparência e prestação de contas como princípios essenciais para moderação de conteúdo, exigindo clareza no tratamento de dados e comprovação de compliance. Contudo, sua aplicação enfrenta desafios práticos ao colidir com segredos comerciais e sistemas automatizados em "caixas-pretas". Para mitigar vieses discriminatórios, a lei prevê auditorias pela ANPD como mecanismo de controle sobre algoritmos de moderação (Franco, 2024, p. 72).

A LGPD constitui-se como o principal marco regulatório atual<sup>76</sup>, criando um sistema abrangente de proteção de dados pessoais e instituindo a Autoridade Nacional de Proteção de Dados<sup>77</sup> (ANPD). À época de sua criação, se deu pelo fato do alto impacto em diversos setores,

---

<sup>75</sup> O artigo 19 do Marco Civil da Internet limita a responsabilidade civil de provedores de aplicações à hipótese de descumprimento de ordem judicial específica para remoção de conteúdo ilícito, medida que visa resguardar a liberdade de expressão e evitar censura prévia; exige-se que a ordem identifique com clareza o material a ser removido, sob pena de nulidade, e ressalva-se que, em casos de violação de direitos autorais, aplica-se legislação específica compatível com os direitos fundamentais, sendo possível o julgamento em juizados especiais e a concessão de tutela antecipada quando presentes prova inequívoca, risco de dano e interesse público, buscando-se o equilíbrio entre direitos individuais e um ambiente digital livre. BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: .29 jun. 2025.

<sup>76</sup> O artigo 6º da Lei Geral de Proteção de Dados (LGPD) elenca os princípios que regem o tratamento de dados pessoais, estabelecendo que “as atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – finalidade (...); II – adequação (...); III – necessidade (...); IV – livre acesso (...); V – qualidade dos dados (...); VI – transparência (...); VII – segurança (...); VIII – prevenção (...); IX – não discriminação (...); X – responsabilização e prestação de contas”, conjunto normativo que fundamenta a interpretação jurídica da proteção de dados no ordenamento brasileiro. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em 14 maio 2025.

<sup>77</sup> A ANPD se configura como entidade autônoma, dotada de características específicas, e encontra-se subordinada ao Ministério da Justiça e Segurança Pública. A atuação da ANPD concentra-se, primordialmente, na garantia da segurança dos dados pessoais. Adicionalmente, compete-lhe estabelecer diretrizes e atos normativos, bem como fiscalizar a efetiva aplicação da LGPD.



sua base nos direitos humanos e a justificativa econômica para sua existência na sociedade digital<sup>78</sup>:

(...) a necessidade de uma lei específica sobre proteção dos dados pessoais decorre da forma como está sustentado o modelo atual de negócios da sociedade digital, na qual a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências. (Pinheiro, 2018, p. 22)

A LGPD então estabeleceu bases sólidas para o tratamento de informações, definindo princípios como finalidade específica, necessidade e transparência, além de prever direitos aos titulares e sanções administrativas para os agentes de tratamento:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional. § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta. § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei. (Brasil, 2018)

Analizando o artigo supracitado, destaca-se que a delimitação de esferas individuais e coletivas, o que implica na existência de uma considerável latitude hermenêutica na subsunção de situações fáticas às normas jurídicas, com vistas à ponderação dos interesses em conflito.

(...) ao mesmo que ele pretende proteger o indivíduo, reconhece que fazemos parte de uma sociedade, a qual se desenvolve, também, pela economia. Portanto, há limites individuais e coletivos, o que significa que existe uma ampla margem interpretativa para uma mesma situação, visando buscar entender os dois lados (Garcia, 2020, p.7).<sup>79</sup>

<sup>78</sup> Evidencia-se que a incidência da LGPD é de âmbito extraterritorial. A norma incide sobre o tratamento de dados realizado fora do Brasil quando a coleta ocorreu no território nacional, ou a oferta de produtos ou serviços se direciona a indivíduos localizados no Brasil ou que nele estiveram. Processamentos em infraestruturas localizadas no exterior, como armazenamento em nuvem, estão, portanto, sujeitos a essa regulação sob tais condições. PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018-LGPD. Saraiva Educação SA, 2018.

<sup>79</sup> GARCIA, Lara Rocha et al. Lei Geral de Proteção de Dados (LGPD): guia de implantação. Editora Blucher, 2020.

Além da norma estabelecer as conceituações de dado pessoal e dado pessoal sensível e define os agentes do tratamento, a saber: o Titular dos dados, o Controlador que toma as decisões, o Operador que processa em nome deste, o Encarregado como canal de comunicação e a ANPD como órgão fiscalizador e regulamentador.

Examinando o regime sancionatório da LGPD (Capítulo VIII), observa-se que a ANPD aplica sanções administrativas por infrações, que variam de advertências e multas a restrições sobre dados e atividades de tratamento; tais penalidades, embora graduadas, podem ser cumulativas, e sua aplicação considera a gravidade da infração, o dano e a conduta do infrator em procedimento administrativo (Brasil, 2018).<sup>80</sup>

A jurisprudência tem desempenhado papel crucial na consolidação desses direitos, como demonstrado em decisões que responsabilizam empresas por falhas na segurança de dados (STJ, REsp 2092096/2023<sup>81</sup>):

Civil, consumidor e processual civil. Ação indenizatória c/c obrigação de fazer. Fornecimento de serviços pela B3 aos investidores fora do âmbito das operações no mercado de capitais. Relação jurídica direta e autônoma de consumo. Incidência do CDC. Plataforma virtual que armazena e utiliza dados pessoais dos investidores. Incidência da LGPD e do marco civil da internet. Acesso não autorizado por terceiros. Exclusão dos dados inseridos indevidamente por terceiros. Possibilidade. 6. No âmbito das operações no mercado de capitais, não incide o CDC na relação jurídica entre o investidor e a B3, que mantém relação exclusiva com corretoras. 7. Contudo, ao disponibilizar plataforma virtual de acesso direto ao investidor (Canal Eletrônico do Investidor), a B3 estabelece relação de consumo autônoma, regida pelo CDC. 8. A B3, ao armazenar e utilizar dados pessoais, submete-se à LGPD. 9-11. O titular dos dados pode exigir correção, bloqueio ou exclusão de dados indevidos, cabendo ao agente de tratamento assegurar segurança conforme arts. 6º, II e VII, e 46 da LGPD. 13. A B3 enquadra-se como provedora de aplicação de internet, sujeita ao Marco Civil da Internet. 14. Condenação da B3 a fornecer registros de acesso não autorizado e excluir dados inseridos por terceiros, afastando-se responsabilidade por danos morais (STJ - REsp: 2092096 SP 2023/0294797-4, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 12/12/2023, T3 - TERCEIRA TURMA, Data de Publicação: DJe 15/12/2023)

<sup>80</sup> Os arts. 52 a 54 da LGPD instituem regime de sanções administrativas aplicáveis pela ANPD em caso de infração, incluindo advertência, multas (simples ou diária), publicização da infração e restrições ao tratamento de dados; tais sanções são impostas após procedimento com ampla defesa, observando critérios como gravidade da infração, boa-fé, vantagem auferida, condição econômica, reincidência, extensão do dano e adoção de medidas corretivas, cabendo à ANPD regulamentar os parâmetros de cálculo das penalidades. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em 14 maio 2025.

<sup>81</sup> BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 2092096, Civil, Consumidor e Processual Civil. Ação Indenizatória C/C Obrigação de Fazer. Relator: Ministra NANCY ANDRIGHI. Brasília, DF, 12 de dezembro de 2023. Brasília, 15 dez. 2023. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28RESP.clas.+e+%40num%3D%222092096%22%29+ou+%28RESP.adj+%222092096%22%29.suce.&O=JT>. Acesso em: 03 abr. 2025.

A análise do regime jurídico do tratamento de dados pessoais na LGPD, notadamente em seu Capítulo II<sup>82</sup>, estabelece a regulação da licitude dessas atividades, indicando o consentimento do titular como base legal preponderante, embora outras hipóteses sejam admitidas, como o legítimo interesse, em correlação com os princípios de fomento ao desenvolvimento econômico e tecnológico (Brasil, 2018).

Destaca-se, ainda, que as responsabilidades legais dos agentes de tratamento não se exaurem pela publicização dos dados pelo titular, e o tratamento de dados sensíveis sem assentimento é circunscrito a exceções legais estritas, como em atividades de pesquisa, exigindo garantias de segurança e vedação de compartilhamento (Garcia, 2020, p. 8).

Já para dados de crianças e adolescentes, impõe-se o consentimento do responsável legal, demandando ainda métodos comunicacionais adequados à sua compreensão, findando-se o tratamento ao ser alcançada a finalidade, expirar o prazo estabelecido, ou por solicitação do titular ou da ANPD (Brasil, 2018).

Apesar da LGPD consolidar-se como pilar essencial para a confiança no ambiente digital brasileiro, persistem desafios significativos, particularmente na harmonização com legislações setoriais e no enfrentamento de incidentes de segurança em larga escala<sup>83</sup>, exigindo constante atualização do marco regulatório para acompanhar a dinâmica evolução tecnológica (Klann, 2020, p. 168).<sup>84</sup>

A interação normativa entre o Decreto n.º 10.332/2020<sup>85</sup>, que impulsiona a digitalização dos serviços públicos, e a Lei n.º 13.709/2018 configura o regime aplicável ao tratamento de dados pessoais no contexto da transformação digital estatal. Enquanto o Decreto fomenta a digitalização, a LGPD disciplina as operações de tratamento de dados a ela inerentes. Consequentemente, as iniciativas de governo digital exigem conformidade integral com os preceitos da LGPD.

---

<sup>82</sup> O artigo 7º da LGPD dispõe sobre as bases legais para o tratamento de dados pessoais, prevendo hipóteses como “I – mediante o fornecimento de consentimento pelo titular; II – para o cumprimento de obrigação legal ou regulatória pelo controlador; (...) X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente”, constituindo rol que reflete a vinculação entre finalidade legítima, interesse público e direitos fundamentais na disciplina da proteção de dados. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 14 maio 2025.

<sup>83</sup> A massa informacional veiculada não guarda correspondência com um volume físico relevante. Este aspecto configura uma particularidade dos dados digitais, visto que quantidades expressivas de informações são processadas ou armazenadas sem a necessidade de suportes materiais tradicionais, tais como papel, rolos ou fitas, entre outros. DATE, C. J. Introdução a Sistemas de Banco de Dados. 8. ed. Rio de Janeiro: Campus, 2003.

<sup>84</sup> KLANN, Clarice. Teoria Geral do Direito Digital. Indaial: Uniassevi, 2020.

<sup>85</sup> BRASIL. Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/decreto/d10332.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm). Acesso em: 24 maio 2025.

A Lei 14.129/2021<sup>86</sup> consolida o marco legal da transformação digital do setor público no Brasil, redefinindo deveres da administração e direitos dos cidadãos em relação ao acesso digital a serviços públicos. Ela reforça os princípios de governo digital inclusivo, transparente e eficiente, com suporte jurídico para inovação e uso ético de tecnologias.

A privacidade, inicialmente balizada pela Constituição de 1988, ganhou contornos normativos com o CDC (1990) e a Lei do *Habeas Data* (1997), embora num cenário anterior à era digital. A LAI (2011) e o MCI (2014) expandiram os princípios de transparência e consentimento, preparando o terreno para a LGPD.

Consolidando -se como um marco regulatório abrangente ao estabelecer princípios como finalidade e segurança, e ao criar a ANPD, a LGPD unificou normas dispersas e respondeu às demandas da era digital. Decisões judiciais (REsp 2092096/2023) demonstram sua aplicação prática, reforçando a proteção dos titulares e a responsabilidade dos agentes.

A LGPD é um pilar crucial para proteger liberdades na sociedade digital de risco, mas esbarra em limitações: a tutela da privacidade mostra-se insuficiente diante de vazamentos, vigilância e segmentação comportamental. Embora seus princípios garantam avanços, a lei requer complementos como regulação penal de dados, políticas públicas educativas e aprimoramento de relatórios de impacto. O equilíbrio entre segurança e liberdade permanece o desafio central, exigindo soluções que evitem a dicotomia pendular entre controle excessivo e exposição vulnerável (Hermes, 2023, p. 180).<sup>87</sup>

### 5.3 Segurança Cibernética

A segurança da informação e a segurança cibernética ganharam relevância no Brasil devido ao crescimento exponencial de ataques digitais, vazamentos de dados e a crescente dependência de infraestruturas críticas interconectadas. Em resposta a esses desafios, o Decreto nº 9.637/2018<sup>88</sup> instituiu a Política Nacional de Segurança da Informação (PNSI),

<sup>86</sup> A Lei nº 14.129/2021, conhecida como Lei do Governo Digital, estabelece princípios e diretrizes para a prestação digital de serviços públicos no Brasil, promovendo eficiência, transparência, acessibilidade e inovação na administração pública. Seu foco é garantir que o cidadão possa acessar serviços públicos pela internet, com menos burocracia e mais agilidade. BRASIL. Lei nº 14.129, de 29 de março de 2021. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2021/lei/14129.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/14129.htm). Acesso em: 19 maio 2025.

<sup>87</sup> HERMES, Pedro Henrique; LEAL, Rogério Gesta. A liberdade digital na Sociedade do Risco: perspectivas a partir da Proteção de Dados Pessoais. Revista Eletrônica Direito & TI, v. 1, n. 16, p. 158-185, 2023.

<sup>88</sup> BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/decreto/d9637.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm). Acesso em: 24 maio 2025.

estabelecendo diretrizes para a proteção de sistemas governamentais e privados contra ameaças físicas e virtuais.

Essa política estrutura-se em três eixos principais, quais sejam:

Segurança cibernética: Prevenção e resposta a incidentes como invasões, ransomware e ataques de negação de serviço (DDoS). Defesa cibernética: Proteção de infraestruturas críticas, como redes de energia, sistemas de saúde e transporte. Gestão de riscos: Adoção de padrões internacionais, como a ISO/IEC 27001, para identificar vulnerabilidades e implementar controles (Brasil, 2018).

Complementando essa base, o Decreto nº 10.222/2020<sup>89</sup> aprovou a Estratégia Nacional de Segurança Cibernética (E-Ciber), com ações específicas para fortalecer a resiliência do país, incluindo a capacitação de profissionais, parcerias público-privadas e a integração com iniciativas globais, como a Convenção de Budapeste sobre Cibercrime. A E-Ciber também reforça a proteção de dados pessoais, alinhando-se à LGPD para mitigar violações que comprometam a privacidade (Brasil, 2020).

No setor financeiro, a Resolução do Conselho Monetário Nacional (CMN) nº 4.658/2018<sup>90</sup> do Banco Central impôs requisitos rigorosos para instituições financeiras, como a adoção de políticas de segurança cibernética, testes de invasão (*pentests*) e planos de contingência ataques (Brasil, 2018).

O estudo de Belli, et al. (2023) realiza uma análise crítica do arcabouço normativo brasileiro concernente à cibersegurança. A pesquisa aponta a ausência de articulação entre este conjunto de normas e outros diplomas legais relevantes para a área, especificamente a LGPD e o MCI<sup>91</sup>:

(...) destaca-se que as normas federais analisadas carecem de coesão textual, conceitual e estrutural quando introduzidas no contexto de outras diretrizes e leis do nosso ordenamento jurídico que abordem temas correlatos. Ilustrativamente, cita-se a ausência de correlação normativa com a Lei nº. 13.709/2018, Lei Geral de Proteção

<sup>89</sup> Constata-se no Decreto nº 10.222/2020 que sua parte normativa compreende apenas três artigos. Em contrapartida, o referido Decreto dispõe de um extenso anexo, apresentado em formato de texto descritivo, o qual contém um vasto conteúdo destinado a pormenorizar a estratégia a que a norma se refere. POLIDO, Fabrício; ANJOS, Lucas (orgs.). Marco Civil e Governança da Internet: diálogos entre o doméstico e o global. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2016. BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/decreto/d10222.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm). Acesso em: 12 maio. 2025.

<sup>90</sup> BRASIL. Conselho Monetário Nacional. Resolução nº 4.658, de 26 de abril de 2018. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Diário Oficial da União, Brasília, DF, 27 abr. 2018. Disponível em: [https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50581/Res\\_4658\\_v1\\_O.pdf](https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf). Acesso em 29 jun. 2025.

<sup>91</sup> BELLI, Luca et al. Cibersegurança. 2023.

de Dados, que, além de regulamentar o tratamento de dados pessoais, nos meios físicos e digitais, pelas pessoas físicas e jurídicas privada e pública (art. 1º) – dimensão da segurança da informação –, introduz a figura do encarregado pelo tratamento de dados (art. 5º, inciso VIII), não incluído nos textos legais analisados, e cria a Autoridade Nacional de Proteção de Dados (ANPD), conforme disposto no artigo 55-A.

Em complemento às lacunas de integração normativa, destaca-se o papel crescente de normas técnicas, como a ABNT NBR ISO/IEC 27002, que oferecem parâmetros operacionais para a efetivação de boas práticas de segurança. Tais diretrizes tornaram-se essenciais para a implementação de controles avançados, como criptografia de dados e autenticação multifatorial, representando um contraponto prático à fragilidade do alinhamento legal:

Art. 2º As instituições referidas no art. 1º devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. § 1º A política mencionada no caput deve ser compatível com: I - o porte, o perfil de risco e o modelo de negócio da instituição; II - a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e III - a sensibilidade dos dados e das informações sob responsabilidade da instituição. § 2º Admite-se a adoção de política de segurança cibernética única por: I - conglomerado prudencial; e II - sistema cooperativo de crédito. Resolução nº 4.658, de 26 de abril de 2018 Página 2 de 11 § 3º As instituições que não constituírem política de segurança cibernética própria em decorrência do disposto no § 2º devem formalizar a opção por essa faculdade em reunião do conselho de administração ou, na sua inexistência, da diretoria da instituição (Brasil, 2018).

A Resolução nº 4.658/2018 destaca a necessidade de políticas de segurança cibernética adaptadas ao perfil de risco de cada instituição, levando em conta o porte, a complexidade operacional e a sensibilidade dos dados tratados. A normativa ainda prevê certa flexibilidade, permitindo que conglomerados prudenciais e sistemas cooperativos adotem políticas unificadas, desde que compatíveis com suas especificidades (Brasil, 2018).

Apesar dessas diretrizes, persistem desafios significativos na prática. Muitos órgãos públicos, especialmente em nível municipal, ainda operam com infraestrutura tecnológica defasada. Além disso, há dificuldade em harmonizar normas técnicas com o ritmo acelerado da inovação digital, gerando lacunas na efetividade das políticas implementadas.

Em resposta a esse cenário, foram adotadas medidas legislativas importantes. Com a sanção da Lei nº 14.155/2021<sup>92</sup>, alteraram-se o Código Penal e o Código de Processo Penal para

<sup>92</sup> BRASIL. LEI Nº 14.155, DE 27 DE MAIO DE 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2021/lei/14155.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/14155.htm). Acesso em 21 maio 2025.

endurecer a repressão aos crimes cibernéticos. A nova lei aumentou penas e introduziu qualificadoras para delitos como furto e estelionato cometidos por meios digitais, além de estabelecer regras específicas de competência para sua persecução.

De maneira complementar, iniciativas estratégicas como o Programa Nacional de Segurança Cibernética<sup>93</sup>, lançado em 2023, visam enfrentar essas lacunas de forma mais ampla. O programa promove investimentos em pesquisa, capacitação nacional e campanhas de conscientização, buscando consolidar um ecossistema digital mais seguro, resiliente e alinhado às exigências da era da informação.

## 5.4 Jogos Eletrônicos

A indústria de jogos eletrônicos no Brasil alcançou um marco regulatório significativo com a Lei nº 14.852/2024<sup>94</sup> (Marco Legal dos Jogos Eletrônicos), que estabeleceu um equilíbrio entre o fomento ao setor e a proteção aos usuários.

Esta legislação reconhece os jogos como obras complexas que integram elementos tecnológicos e artísticos, exigindo uma abordagem jurídica multifacetada que combina a proteção do *software* com salvaguardas adicionais para componentes criativos através do direito autoral (Lei nº 9.610/1998).

Impulsionados pelo progresso tecnológico, os jogos eletrônicos surgiram como obras complexas que mesclam elementos artísticos e o programa de computador, constituindo um setor econômico global e brasileiro de notável crescimento e relevância. Dada a natureza imaterial predominante desta indústria, a propriedade intelectual é essencial para sua estrutura

---

<sup>93</sup> A segurança cibernética nos órgãos públicos municipais enfrenta desafios como infraestrutura obsoleta e dificuldade de alinhar normas técnicas à inovação; nesse cenário, o Programa Nacional de Segurança Cibernética busca mitigar tais fragilidades, sendo que as normas ABNT NBR ISO/IEC 27001 e 27002 oferecem diretrizes fundamentais para a gestão da segurança da informação, servindo como base estratégica para a modernização institucional e a resiliência digital. BRASIL. Associação Brasileira De Normas Técnicas (ABNT). ABNT NBR ISO/IEC 27001: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022a. BRASIL. Associação Brasileira De Normas Técnicas (ABNT). ABNT NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. Rio de Janeiro: ABNT, 2022b.

<sup>94</sup> Para Salen e Zimmerman, o jogo eletrônico é definido como atividade interativa mediada por dispositivo computacional que executa programa com regras e objetivos, voltada ao entretenimento, aprendizado ou simulação; nos termos do artigo 5º da legislação aplicável, abrange: I – obra audiovisual interativa em forma de programa de computador, conforme a Lei nº 9.609/98, com imagens alteradas em tempo real pelas ações do jogador; II – dispositivo central e acessórios cuja principal função é executar jogos eletrônicos; III – software operável em dispositivos móveis, páginas web ou consoles, incluindo jogos em realidade virtual, aumentada, mista ou estendida, independentemente da forma de consumo. SALEN, Katie; ZIMMERMAN, Eric. Rules of Play: Game Design Fundamentals. Cambridge: MIT Press, 2004.

jurídica e gestão, conferindo proteção tanto ao *software* quanto aos componentes artísticos individuais sob legislação específica e direitos autorais (Romão, 2019, p.3).

Os jogos eletrônicos, obras complexas que integram arte e tecnologia, impõem desafios significativos em propriedade intelectual devido à sua natureza transversal e às variadas classificações legais adotadas globalmente.

O arcabouço legal brasileiro é bastante taxativo quando se trata dessa modalidade contratual aliada à diversão. Há regulamentação no Código Civil, como se verá adiante, na Lei das Contravenções Penais, no Direito Empresarial e em diversos decretos constantes da legislação ordinária.

A normatização das apostas online e jogos de azar no Brasil exibiu, antes da Lei n.º 14.790/2023, notável ambiguidade, suscitando questionamentos sobre a legalidade da prática e a aplicabilidade do CDC aos apostadores. Embora a Lei n.º 14.790 tenha promovido a regulamentação parcial do setor, o seu artigo 27 expressamente estende aos apostadores das modalidades normatizadas a garantia dos direitos consumeristas previstos no CDC (Santos; Coelho; Bernardes, 2025, p. 3410).<sup>95</sup>

Embora a tendência majoritária os associe ao *software*, elementos audiovisuais e literários são distintivos e passíveis de proteção por direitos autorais, sendo que no Brasil a proteção se estende ao *software* pela legislação específica e aos elementos criativos por direitos autorais, além da aplicabilidade de marcas e segredos comerciais. Dada a natureza imaterial e a rápida evolução da indústria, a propriedade intelectual é crucial para a apropriabilidade e gestão dos jogos, fomentando o desenvolvimento tecnológico e a difusão cultural (Romão, 2019, p.12).

O Marco Legal trouxe avanços importantes ao garantir liberdade para produção e comercialização, desde que observada a classificação etária e implementados mecanismos de controle parental, especialmente para proteger o público infantil:

Art. 1º Esta Lei cria o marco legal para a indústria de jogos eletrônicos. Art. 2º A fabricação, a importação, a comercialização, o desenvolvimento e o uso comercial de jogos eletrônicos são regulados por esta Lei. Art. 3º São livres a fabricação, a importação, a comercialização, o desenvolvimento e o uso comercial de jogos eletrônicos, observado o disposto no art. 173 da Constituição Federal e na legislação vigente. § 1º O Estado realizará a classificação etária indicativa, dispensada autorização estatal prévia para o desenvolvimento e a exploração dos jogos eletrônicos abrangidos por esta Lei. § 2º Na realização da classificação etária indicativa de jogos

<sup>95</sup> SANTOS, Gabrielly Cordeiro dos; COELHO, Ivana Lara Ribeiro; BERNARDES, Rochele Juliane Lima Firmeza. Entre a diversão e a ruína: a influência das apostas online/bets no endividamento excessivo do brasileiro. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 11, n. 4, p. 3396-3420, 2025.



eletrônicos, levar-se-ão em conta os riscos relacionados ao uso de mecanismos de microtransações (Brasil, 2024).

Além de assegurar a liberdade de desenvolvimento, a norma também inovou ao criar incentivos fiscais e linhas de crédito específicas, equiparando a indústria de games ao setor cultural. Essas medidas visam fomentar o empreendedorismo, estimular a produção de conteúdos regionais e educativos, e fortalecer a economia criativa no Brasil.

Um ponto de destaque foi a clara distinção entre jogos de entretenimento e apostas eletrônicas<sup>96</sup> (*eSports betting*), estas últimas submetidas a regulação mais rigorosa através das Leis nº 13.756/2018 e 14.790/2023.<sup>97</sup>

Apesar desses avanços, desafios relevantes persistem, principalmente no que se refere a mecânicas como as *loot boxes*<sup>98</sup> sistemas de recompensas aleatórias que levantam preocupações sobre seu potencial aditivo e falta de transparência. O debate jurídico e ético sobre sua regulamentação ainda está em aberto e exige atenção contínua.

Nesse cenário, o papel da ANPD torna-se central ao fiscalizar o uso e o tratamento de informações pessoais nos jogos online. Simultaneamente, iniciativas como o Plano Brasileiro de IA abrem espaço para inovações tecnológicas, como narrativas adaptativas e personagens controlados por IA, reforçando a necessidade de um arcabouço ético e seguro.

Essa evolução normativa e institucional evidencia a maturidade crescente do setor de jogos eletrônicos no país, revelando esforços para equilibrar o desenvolvimento econômico e tecnológico com a proteção de direitos fundamentais, como a privacidade e o consumo responsável.

Em investigação econômica do setor de jogos digitais no Brasil, balizada pelos instrumentos da Análise Econômica do Direito (AED) e da Análise de Impacto Regulatório

<sup>96</sup> As apostas eletrônicas, também denominadas *eSports betting*, verifica-se que estas consistem em apostas realizadas no âmbito de competições de jogos eletrônicos, conhecidos como *eSports* (esportes eletrônicos). Esta modalidade configura um segmento em expansão no mercado de apostas online, no qual os apostadores efetuam previsões sobre os resultados de partidas de videogames disputadas em nível profissional.

<sup>97</sup> O artigo 2º da Lei nº 14.790/2023 define, para fins de aplicação, termos como “aposta”, entendida como ato de risco com expectativa de prêmio; “quota fixa”, fator multiplicador do valor apostado; “apostador”, pessoa física que aposta; distingue apostas físicas (por bilhete impresso) e virtuais (realizadas por canais eletrônicos controlados pelo operador); prevê também conceitos como “evento real de temática esportiva”, “jogo on-line”, “evento virtual de jogo on-line”, “agente operador de apostas”, e “aplicações de internet” como base terminológica da regulação do setor. BRASIL. Lei nº 14.790, de 29 de dezembro de 2023. Dispõe sobre a modalidade lotérica denominada apostas de quota fixa; altera as Leis nºs 5.768, de 20 de dezembro de 1971, e 13.756, de 12 de dezembro de 2018, e a Medida Provisória nº 2.158-35, de 24 de agosto de 2001; revoga dispositivos do Decreto-Lei nº 204, de 27 de fevereiro de 1967; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2023/lei/14790.htm](https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/14790.htm). Acesso em: 6 de abr. de 2025.

<sup>98</sup> Conforme Zendle, Meyer e Over, “as loot boxes são uma forma relativamente nova para os jogadores gastarem dinheiro em videogames”. ZENDLE, David; MEYER, Rachel; OVER, Harriet. *Adolescentes e loot boxes: Ligações com jogo problemático e motivações para compra*. Royal Society open science, v. 6, n. 6, p. 190049, 2019.

(AIR), Schmidt, Amaral e Couto (2024, p. 115) examinam as dinâmicas de mercado e os efeitos da legislação, com especial atenção ao Marco Legal dos Games (Lei nº 14.852/2024).

Nesse contexto, a AED permite aferir a eficiência das mudanças normativas e comparar cenários regulatórios distintos, enquanto a AIR analisa os custos e benefícios das regulações propostas. A aplicação conjunta desses métodos revelou uma questão estrutural: a deficiência histórica no incentivo e na articulação estatal com o setor de jogos, o que contrasta fortemente com seu expressivo potencial econômico. Segundo dados levantados pelos autores<sup>99</sup>:

No Brasil, a receita total de jogos digitais e e-sports — sendo este conceituado por Minamihara (2020, p. 24) como “a profissionalização das competições de jogos eletrônicos, trazendo um paralelo com os esportes tradicionais” — no ano de 2021 foi de US\$ 1,4 bilhão e deve ultrapassar US\$ 2,8 bilhões em 2026, aumentando em um CAGR (taxa de crescimento anual composta) de 15,2% e responderá até 2026 na América Latina por 47,4% da receita total do mercado de jogos digitais (Schmidt; Amaral; Couto, 2024, p.114).

Diante desse cenário promissor, o Brasil tem avançado na proteção jurídica e na promoção da criatividade, estruturando um ambiente legal que busca equilibrar os direitos autorais e a legislação de software no contexto dos jogos eletrônicos. No entanto, é fundamental que as políticas públicas continuem evoluindo em sintonia com os avanços tecnológicos, evitando tanto a omissão quanto os excessos regulatórios, sobretudo no tocante à proteção de públicos vulneráveis.

Outro ponto relevante diz respeito à distinção normativa entre jogos de entretenimento e apostas eletrônicas, que requer fiscalização rigorosa para mitigar riscos à integridade do consumidor. Paralelamente, a atuação da Autoridade Nacional de Proteção de Dados (ANPD) e a incorporação de princípios éticos no uso da IA em jogos representam pilares fundamentais para garantir um ecossistema digital inovador, mas também seguro e orientado à proteção de dados.

---

<sup>99</sup> A análise econômica do setor no Brasil, feita por Schmidt, Amaral e Couto (2024, p.115) indica uma movimentação financeira anual de R\$ 13 bilhões, mesmo na carência de uma política nacional formal. Projeta-se que o Marco Legal dos Games (MLG) contribua para o posicionamento competitivo do país no cenário global. SCHMIDT, Albano Francisco; AMARAL, Luise; COUTO, Vanessa Ribeiro. Marco Legal dos Games: análise exploratória do cenário econômico dos jogos digitais e sua relevância para a economia brasileira. 2024.

## 5.5 Regulação do Poder Econômico Digital

A regulação do poder econômico no cenário digital brasileiro evidencia complexidades singulares, sobretudo em face do crescimento exponencial de plataformas tecnológicas que alcançaram proporções sistêmicas.

Nesse cenário, a análise de Manuel Castells (1999, p. 567)<sup>100</sup> sobre a dinâmica do poder na sociedade em rede é particularmente relevante: “os conectores são os detentores do poder. Uma vez que as redes são múltiplas, os códigos interoperacionais e as conexões entre redes tornam-se as fontes fundamentais da formação, orientação e desorientação das sociedades”.

Em vigor desde junho de 2023, a Lei n.º 14.478/2022<sup>101</sup> instituiu o marco regulatório para o mercado de criptoativos no Brasil. O diploma legal objetiva conferir maior segurança jurídica, transparência e proteção aos consumidores, ao definir os requisitos e princípios para a operação dos prestadores de serviços de ativos virtuais. Esta regulamentação insere o setor no âmbito do sistema jurídico e financeiro nacional.

O arcabouço legal atual, fundamentado principalmente na Lei de Defesa da Concorrência, mostra-se desafiado por novas realidades como os algoritmos de precificação e os ecossistemas digitais fechados. Esta legislação, embora abrangente ao tipificar condutas anticompetitivas com base em seus efeitos (independentemente de culpa ou resultados concretos), necessita de constante reinterpretação para acompanhar a dinâmica dos mercados digitais (Frazão; Goettenauer, 2022, p. 23).<sup>102</sup>

O judiciário brasileiro tem enfrentado casos que ilustram essas tensões. Em decisão recente (REsp n. 1.836.349/SP<sup>103</sup>), o Superior Tribunal de Justiça manteve entendimento de que plataformas digitais que atuam como meros “classificados online” não respondem por transações fraudulentas realizadas por terceiros em seus ambientes virtuais, desde que comprovada a ausência de intermediação direta. Este posicionamento reflete os limites da responsabilização desses agentes econômicos sob a legislação atual:

<sup>100</sup> CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 1999. v. 1.

<sup>101</sup> BRASIL. Lei n.º 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2022/lei/l14478.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm). Acesso em: 24 maio 2025

<sup>102</sup> FRAZAO, Ana Oliveira; GOETTENAUER, Carlos. Algoritmos de precificação e direito concorrencial. Revista Eletrônica do Curso de Direito da UFSM, v. 17, n. 1, p. e40973-e40973, 2022.

<sup>103</sup> BRASIL. Superior Tribunal de Justiça. Recurso Especial n.º 1.836.349/SP. Relator: Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 21 jun. 2022. Diário da Justiça Eletrônico, DJe de 24 jun. 2022. Disponível em: [https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2181939&nu\\_m\\_registro=201901346226&data=20220624&formato=PDF](https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2181939&nu_m_registro=201901346226&data=20220624&formato=PDF). Acesso em 24 maio 2025.

Direito do consumidor. Golpe através de anúncio online. Ausência de responsabilidade da rede social e do banco de origem da transação. Recurso não provido. I. Caso em exame. 1) Recurso inominado interposto pela parte reclamante contra a sentença que julgou improcedentes os pedidos indenizatórios em razão de golpe sofrido pela autora. A parte reclamante asseverou a culpa da reclamada Facebook pois atua como marketplace, e da corré Nubank pois não tomou medidas para solucionar o problema após a contestação. II. Questão em discussão. 2) As questões em discussão consistem em: (i) saber se há responsabilidade do Facebook por golpes sofridos em anúncios em sua plataforma; (ii) saber se há responsabilidade do Nubank por transações feitas pela autora em contexto de golpe. III. Razões de decidir. 3) Não há prova do anúncio realizada na plataforma reclamada. Mesmo que houvesse, o réu Facebook atua como mero “classificados” online, não sendo responsável por transações que não tenha intermediado. 4) O réu Nubank foi o banco de origem da operação realizada pela parte reclamante, e acionou o sistema MED tempestivamente quando avisado do golpe. Não há responsabilidade quando atua de forma diligente como no caso dos autos. IV. Dispositivo e tese Recurso inominado conhecido e não provido. Sentença mantida. Jurisprudência relevante citada (STJ - Terceira Turma, REsp n. 1.836.349/SP, Rel.: Ministro Marco Aurélio Bellizze, J. 21/6/2022, DJe de 24/6/2022; TJPR - 3ª Turma Recursal, Recurso Inominado, 0043830-31.2023.8.16.0182, Rel.: Juiz de Direito da Turma Recursal dos Juizados Especiais Juan Daniel Pereira Sobreiro, J. 11.08.20242.)

Estudos do Ministério da Fazenda têm apontado lacunas regulatórias significativas, sobretudo em relação aos chamados ecossistemas digitais fechados, nos quais grandes plataformas exercem controle simultâneo sobre infraestrutura crítica, serviços complementares e grandes volumes de dados de usuários. Esse domínio concentrado levanta preocupações quanto à concorrência, à neutralidade da rede e à autonomia dos consumidores.

Como resposta a esse cenário, tem-se proposto a identificação de plataformas com “relevância sistêmica”, que seriam submetidas a obrigações regulatórias específicas, tais como interoperabilidade técnica e compartilhamento controlado de dados não pessoais. Essas medidas visam impedir práticas de autobenefício, garantir concorrência leal e estimular inovação em ambientes digitais.

O Conselho Administrativo de Defesa Econômica<sup>104</sup> iniciou investigações contra plataformas de streaming por suposto favorecimento de conteúdo próprio, além de apurar práticas restritivas em aplicativos de entrega (delivery). Paralelamente, a Autoridade Nacional de Proteção de Dados (ANPD) tem combatido o uso anticompetitivo de dados pessoais, como no caso da personalização abusiva de preços, conhecida como *price discrimination*.<sup>105</sup>

<sup>104</sup> O CADE tem atuado na regulação de plataformas digitais com foco na preservação da concorrência e proteção do consumidor, investigando, entre outros casos, condutas da Google relativas ao Android e à Play Store por possível fechamento de mercado; da c quanto a restrições na App Store e suposto favorecimento ao Apple Pay em detrimento do Mercado Pago, em representação formulada pelo Mercado Livre; e do iFood, por práticas potencialmente excludentes no setor de entregas online, apurando-se impactos à livre concorrência e à escolha do consumidor.

<sup>105</sup> Segundo Elegido, a discriminação de preços consiste na prática de aplicar valores distintos para o mesmo produto ou serviço a diferentes consumidores. Embora frequentemente percebida como iníqua, a discriminação de

Ainda que a Lei nº 14.478/2022 represente um avanço ao disciplinar aspectos dos ativos digitais, o cenário atual evidencia a urgência de mecanismos mais ágeis e eficazes para lidar com fenômenos complexos, como algoritmos de precificação dinâmica e infraestruturas digitais integradas. A jurisprudência começa a delimitar a responsabilidade das plataformas, mas permanece a necessidade de critérios objetivos e transparentes para atribuição de deveres regulatórios.

Em síntese, a regulação do poder econômico digital exige uma abordagem multidisciplinar e integrada, articulando o trabalho de órgãos como o CADE e a ANPD com a participação ativa de setores público, privado e da sociedade civil. Apenas por meio desse diálogo contínuo será possível garantir um ambiente digital equitativo, inovador e competitivo.

## 5.6 Inteligência Artificial

O Plano Brasileiro de Inteligência Artificial (PBIA), lançado no corrente ano pelo Governo Federal, por meio do Ministério da Ciência, Tecnologia e Inovação (MCTI), define inteligência artificial:

como o conjunto de modelos, algoritmos, técnicas e metodologias que podem ser implementados como sistemas computacionais que produzem resultados como previsões, classificações, recomendações e decisões, a partir de processos de aprendizagem baseados em grande volume de dados, com potencial para influenciar ambientes físicos e virtuais.<sup>106</sup>

Para entender o funcionamento desses sistemas, Barbosa e Pinheiro (2023, p. 13) explicam que a IA pode aprender por meio de dois principais métodos: o aprendizado supervisionado e o não supervisionado. A distinção entre ambos está na forma como os dados são apresentados ao sistema:

De forma simplificada, pode-se dizer que a principal diferença é que na primeira forma se utilizam dados rotulados (com informações previamente indicadas) para ajudar a orientar os resultados da análise ou do tratamento desses dados pela IA; em contrapartida, na segunda os dados não são previamente rotulados e, portanto, caberá unicamente ao sistema de IA identificar padrões nos dados brutos fornecidos.<sup>107</sup>

---

preços pode, em certas circunstâncias, fomentar uma melhoria do bem-estar social, inclusive para todas as partes envolvidas na transação. ELEGIDO, Juan M. A ética da discriminação de preços. *Business Ethics Quarterly*, v. 21, n. 4, p. 633-660, 2011.

<sup>106</sup> Ministério Da Ciência, Tecnologia E Inovação - MCTI; Centro De Gestão E Estudos Estratégicos - CGEE. IA para o bem de todos; Plano Brasileiro de Inteligência Artificial. Brasília, DF: MCTI;CGEE, 2025. 104p.

<sup>107</sup> BARBOSA, Leonardo Figueiredo; PINHEIRO, Caroline da Rosa. Inteligência artificial no Brasil: avanços regulatórios. *Revista de Informação Legislativa*, v. 60, n. 240, p. 11-41, 2023.

Esse aprofundamento técnico dialoga diretamente com os objetivos do PBIA, intitulado “IA para o Bem de Todos”, que visa posicionar o Brasil na vanguarda da inovação, sem perder de vista os compromissos com o uso ético, responsável e inclusivo da tecnologia. Conduzida em parceria com o Centro de Gestão e Estudos Estratégicos (CGEE), a estratégia busca alinhar o desenvolvimento da IA com os valores sociais, a diversidade cultural e as prioridades nacionais, promovendo uma aplicação consciente da IA no país.

Para transformar esses princípios em ações concretas, o plano prevê investimentos de R\$ 23 bilhões até 2028, distribuídos em cinco eixos estruturantes: fortalecimento da infraestrutura computacional (com destaque para a criação de supercomputadores de classe mundial e uma “nuvem soberana” de dados); formação e capacitação de profissionais; uso da IA na melhoria de serviços públicos essenciais, como saúde e educação; estímulo à inovação empresarial; e construção de um marco regulatório ético (MCTI, 2025, p. 5).

Apesar da ambição estratégica, o PBIA reconhece os desafios estruturais que o Brasil enfrenta para competir globalmente. Embora o país tenha destaque em produção acadêmica na área, registra apenas 0,2% das patentes globais em IA e sofre com a evasão de talentos, cerca de 78% dos doutores formados no Brasil migram para o exterior. Esse descompasso se intensifica diante do domínio industrial privado (com 70% dos modelos de IA sob controle corporativo) e da baixa adoção da tecnologia entre empresas nacionais, especialmente entre micro, pequenas e médias, das quais apenas 11% utilizam IA em seus processos (MCTI, 2025, p. 22).

Diante desse quadro, o plano propõe medidas emergenciais para reverter o cenário. Entre elas destacam-se: a expansão da infraestrutura de computação de alto desempenho; a criação de polos de inovação setoriais; um programa nacional de retenção de talentos; uma regulação adaptativa baseada em governança ética; e a integração obrigatória de IA nos serviços públicos até 2027, meta considerada estratégica, sobretudo porque 70% do Judiciário já a utiliza, enquanto apenas 5% do Executivo a implementou até agora (MCTI, 2025, p. 23).

Por fim, mesmo com os avanços tecnológicos e institucionais, permanecem importantes dilemas éticos e jurídicos. A IA é uma tecnologia profundamente disruptiva, com potencial para transformar setores inteiros por meio da automação e da predição. No entanto, sua opacidade algorítmica, a dificuldade de responsabilizar decisões automatizadas e a classificação de sistemas como segredos de Estado ou de negócio impõem sérios obstáculos à transparência e à regulação. Nesse contexto, o Brasil começa a estruturar seu marco regulatório,

buscando equilibrar o incentivo à inovação com a garantia dos direitos fundamentais (Frazão; Oliva; Tepedino, 2020, p. 74).

A ética<sup>108</sup> define condutas moralmente adequadas, sendo um elemento central no desenvolvimento de tecnologias emergentes como a IA. No campo da IA, seu papel é assegurar que o avanço técnico esteja alinhado com princípios humanistas e sociais. Em 2021, a UNESCO estabeleceu diretrizes éticas globais para o uso responsável da IA, contemplando valores como transparência, justiça e respeito à privacidade. A urgência desse debate foi reforçada por relatório técnico sobre o GPT-4, que evidenciou riscos concretos associados a grandes modelos linguísticos, incluindo capacidade para engenharia social, exploração de vulnerabilidades cibernéticas e manipulação de usuários (Bueno; Santos, 2024, p.126).

No plano normativo brasileiro, esse esforço ético se reflete na proposta do Projeto de Lei nº 21/2020, cujo Artigo 2º define juridicamente o que se entende por Sistema de Inteligência Artificial (SIA). Segundo o dispositivo, configura-se como SIA o sistema computacional que, orientado por objetivos humanos, demonstra aptidão para aprender, perceber, interpretar e interagir com o ambiente externo por meio do tratamento de dados. A definição inclui técnicas como aprendizado de máquina e abordagens estatísticas, excluindo expressamente sistemas de automação simples que não envolvem capacidade de aprendizado (Brasil, 2020).

Complementando o arcabouço ético e normativo, o Estado brasileiro também tem buscado estruturar um ecossistema de inovação robusto, capaz de impulsionar o desenvolvimento seguro e responsável da IA. Um exemplo disso é a Portaria MCTI nº 4.979/202<sup>109</sup> que estabelece critérios para o credenciamento de Instituições Científicas, Tecnológicas e de Inovação (ICTs), públicas e privadas. A norma operacionaliza as Leis n.º 11.196/2005 (Lei do Bem)<sup>110</sup> e n.º 10.973/2004 (Lei de Inovação), definindo os requisitos para

<sup>108</sup> A ética em IA não diz respeito à tecnologia (incapaz de juízos morais), mas às pessoas que a criam e usam. Como ferramenta, seus impactos dependem da ação humana. Assim, a ética traduz-se na responsabilidade de desenvolvedores, gestores e usuários em garantir que a IA seja programada e aplicada de modo a beneficiar a sociedade, prevenir danos e respeitar direitos fundamentais. GARCIA, Ana Cristina Bicharra. Ética e inteligência artificial. *Computação Brasil*, n. 43, p. 14-22, 2020.

<sup>109</sup> A E-Digital constitui um plano para coordenar as iniciativas governamentais correlatas sob uma perspectiva unificada. Seus objetivos incluem o fomento à digitalização dos processos produtivos, a capacitação para o ambiente digital, a promoção da geração de valor e o estímulo ao crescimento econômico. Neste contexto estratégico, a Inteligência Artificial figura como tecnologia fundamental para a consecução das ações planejadas na transformação digital. BRASIL. *Estratégia Brasileira Para a Transformação Digital (E-Digital)*. Disponível em: [https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-portaria\\_mcti\\_4-979\\_2021\\_anexo1.pdf](https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-portaria_mcti_4-979_2021_anexo1.pdf). Acesso em: 15 maio 2025. BRASIL. Ministério da Ciência, Tecnologia e Inovação. Portaria MCTI nº 4.979, de 2021. Altera o anexo da Portaria MCTI nº 4.617, de 6 de abril de 2021. Disponível em: [https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-portaria\\_mcti\\_4-979\\_2021\\_anexo1.pdf](https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-portaria_mcti_4-979_2021_anexo1.pdf). Acesso em: 24 maio 2025.

<sup>110</sup> BRASIL. Lei nº 11.196, de 21 de novembro de 2005. Institui o Regime Especial de Tributação para a Plataforma de Exportação de Serviços de Tecnologia da Informação – REPEs, o Regime Especial de Aquisição de Bens de

a participação dessas entidades em projetos de Pesquisa, Desenvolvimento e Inovação (PD&I) e a aplicação dos incentivos fiscais correspondentes, com vistas ao fortalecimento do ecossistema de inovação nacional.

Constata-se que a normatização da IA apresenta complexidades significativas. Estes desafios regulatórios decorrem da natureza intrínseca dos algoritmos e dos sistemas de IA, demandando estudo aprofundado e abordagens regulatórias específicas.

Se por um lado a inteligência artificial gera facilidades e viabiliza uma maior difusão de informação, por outro fecunda novas formas de poder inéditas, pois muito embora os detentores de poder econômico sempre tenham tido influência política e mesmo poder de submissão dos indivíduos, essa capacidade de submissão sempre foi circunscrita a um número determinado de pessoas, ainda que fossem muitas, mas jamais na extensão do poder atualmente detido pelas empresas que atualmente dominam o mercado tecnológico, conhecidas como as “big five” (Google, Apple, Microsoft, Facebook e Amazon) com influência política em nível global e poder sobre o comportamento e direitos de pessoas de diferentes países, de maneira que seu poder não conhece conformação ou limitação territorial e desafia a própria soberania dos Estados (Filho; Ladeira, 2021, p. 90).<sup>111</sup>

De acordo com Barbosa e Pinheiro (2023, p.19) a regulação da IA enfrenta desafios estruturais: sua natureza disruptiva exige equilíbrio entre controle de riscos, alocação de custos e promoção da inovação. Problemas práticos incluem a definição imprecisa da tecnologia, a difusão de desenvolvimento (com responsabilidade fragmentada), a opacidade algorítmica e a imprevisibilidade de sistemas autônomos. Modelos regulatórios como o europeu propõem abordagem baseada em risco, flexível para adaptação tecnológica, mas rígida em requisitos essenciais, visando segurança jurídica sem asfixiar a evolução tecnológica.<sup>112</sup>

Os desafios apresentados demonstram, por um lado, a necessidade de estabelecer regramentos para a utilização de sistemas de IA, pois, embora tal tecnologia traga possibilidades de benefícios expressivos para toda a sociedade, ficam evidentes os potenciais riscos da ausência de qualquer regulação. Todavia, eventuais normatizações precisam tomar os devidos cuidados tanto para não desestimular o processo de inovação quanto para minimizar o quantitativo e a gravidade dos riscos e danos aos indivíduos e à sociedade por meio de uma adequada alocação de custos e responsabilidades (Barbosa; Pinheiro; 2023, p. 20).

---

Capital para Empresas Exportadoras – RECAP e o Programa de Inclusão Digital; dispõe sobre incentivos fiscais para a inovação tecnológica. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2004-2006/2005/lei/111196.htm](https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/111196.htm). Acesso em: 24 maio 2025.

<sup>111</sup> FILHO, Marco Aurélio Florêncio; LADEIRA, Fernando. Cidadania digital ou ditadura algorítmica? Contradições do mundo digitalizado e os desafios da regulação. *Duc In Altum-Cadernos de Direito*, v. 13, n. 31, 2021.

<sup>112</sup> BARBOSA, Leonardo Figueiredo; DA ROSA PINHEIRO, Carolina. Inteligência artificial no Brasil: avanços regulatórios. *Revista de Informação Legislativa*, v. 240, pág. 11-41, 2023.



A regulação global da IA consolidou-se em *frameworks* (estrutura) principiológicos, destacando-se a Recomendação da OCDE como paradigma norteador. Seus cinco pilares: crescimento inclusivo, centralidade humana, transparência, robustez e prestação de contas. Esta abordagem flexível, implementada mediante cooperação transfronteiriça e adaptação política contínua, visa equilibrar inovação com mitigação de riscos em cenários de rápida mutação tecnológica (Barbosa; Pinheiro, 2023, p. 25).

Apesar do consenso em torno de princípios gerais, a regulação global da IA enfrenta divergências significativas. Conforme destacam Filho e Ladeira (2021, p. 93), os Estados Unidos e China priorizam a aceleração tecnológica com menor ênfase regulatória, enquanto a União Europeia se destaca por adotar padrões éticos humanocêntricos, como expresso na Carta de Direitos Digitais de 2020. Essa fragmentação é agravada pelo descompasso estrutural entre os sistemas jurídico e tecnológico, o primeiro opera com a lógica binária do lícito/ilícito, enquanto o segundo evolui com base em códigos e linguagens próprias.

Ainda, segundo Filho e Ladeira (2021) esse dilema é aprofundado sob a ótica sistêmica da teoria de Luhmann e Teubner, que afirmam que sistemas autônomos como o jurídico, o econômico e o tecnológico não se comunicam diretamente, mas apenas se “irritam” mutuamente. Ou seja, os direitos fundamentais aplicados à IA não impõem controle direto, mas funcionam como estímulos internos ao sistema tecnológico, induzindo sua autorregulação ética e freando sua expansão descontrolada (Filho; Ladeira, 2021, p. 93).

Nesse cenário, embora o Poder Legislativo seja formalmente a instância primária para a elaboração de normas, a regulação da IA demanda estratégias híbridas e multissetoriais. Como observam Bueno e Santos (2024, p. 114), os desafios são inúmeros: a amplitude das aplicações da IA, a velocidade exponencial de seu desenvolvimento, que frequentemente ultrapassa a capacidade de resposta dos sistemas jurídicos, e a baixa compreensão pública sobre seus impactos. Esses fatores dificultam a formulação de políticas eficazes e indicam a necessidade de modelos regulatórios dinâmicos e adaptativos.<sup>113</sup>

O Brasil encontra-se em fase inicial de estruturação de seu marco regulatório para IA<sup>114</sup> buscando equilibrar o estímulo à inovação tecnológica com a proteção de direitos fundamentais e valores éticos.

<sup>113</sup> BUENO, Eric Fiuza; SANTOS, Marcelo Fonseca. Inteligência Artificial: Desafios Para Regulação Jurídica. Direito & TI, [S. l.], v. 1, n. 18, p. 112–139, 2024. DOI: 10.63451/ti.v1i18.175. Disponível em: <https://direitoeti.com.br/direitoeti/article/view/175>. Acesso em: 20 jun. 2025.

<sup>114</sup> Para Müller e Silveiras (2023), a inteligência Artificial (IA) constitui uma área de pesquisa dedicada ao desenvolvimento de sistemas computacionais aptos a executar atividades que, usualmente, requerem capacidades intelectuais humanas. Tais atividades abrangem o reconhecimento de voz, a visão computacional, a captação e interpretação de dados, bem como o processo de tomada de decisão. MÜLLER, William; SILVEIRAS, Raphael.

O cenário jurídico brasileiro, em sintonia com a tendência internacional, tem apresentado iniciativas crescentes para a regulação da inteligência artificial. Diversas propostas legislativas tramitam nas duas casas do Congresso Nacional com o objetivo de estabelecer princípios, políticas públicas e diretrizes que orientem o desenvolvimento e o uso ético da IA no país.

Em paralelo às movimentações legislativas, o Poder Executivo também tem atuado de forma proativa. Em 2021, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) lançou a Estratégia Brasileira de Inteligência Artificial (EBIA), como desdobramento da Estratégia Brasileira para a Transformação Digital (2018).

A EBIA contempla o fomento a centros de pesquisa aplicada e ações voltadas à inovação tecnológica. Contudo, na ausência de uma legislação específica sobre IA, a regulação atual se apoia em normas preexistentes, como a Lei Geral de Proteção de Dados (LGPD) e dispositivos do direito civil e consumerista, que incidem de forma transversal sobre os sistemas inteligentes (Barbosa; Pinheiro, 2023, p. 27).

Mais recentemente, dois projetos de lei em tramitação no Congresso Nacional, o PL 21/2020<sup>115116</sup> e o PL 2338/2023<sup>117</sup> delineiam os primeiros contornos dessa regulamentação. O primeiro estabelece princípios basilares como transparência, não-discriminação e responsabilização por danos, enquanto o segundo avança na criação de um órgão regulador

---

A Evolução e a Regulamentação da Inteligência Artificial no Brasil. Revista InterCiência-IMES Catanduva, v. 1, n. 11, p. 2-2, 2023.

<sup>115</sup> De acordo com Barbosa e Pinheiro (2023) “a despeito de o PL no 21/2020 ter avançado numa conceituação mais ampla, mencione-se o esforço para a definição de IA apresentada pela minuta do substitutivo (art. 4º), na qual se verifica um conceito mais amplo e principiológico, tendente a compatibilizar-se com marcos regulatórios setoriais. Contudo, ressalva-se o tratamento da IA de forma genérica devido aos riscos de superposições ou conflitos regulatórios, e defende-se como solução alguma forma de coordenação geral entre os setores”. BARBOSA, Leonardo Figueiredo; PINHEIRO, Caroline da Rosa. Inteligência artificial no Brasil: avanços regulatórios. Revista de Informação Legislativa, v. 60, n. 240, p. 11-41, 2023.

<sup>116</sup> O PL 21/2020 estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil, e dá outras providências. Esse PL, em tramitação no Congresso Nacional, propõe a instituição de um marco legal para o uso da inteligência artificial (IA) no Brasil. Este instrumento normativo estabelece princípios, direitos, deveres e mecanismos de governança aplicáveis a todos os atores envolvidos, públicos e privados, visando a equilibrar o fomento à inovação tecnológica com a garantia de direitos e a gestão de riscos inerentes aos sistemas de IA. Sua finalidade precípua é promover o desenvolvimento ético e responsável da IA no país. BRASIL. Projeto de Lei nº 21/2020. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2236340>. Acesso em: 12 maio 2025.

<sup>117</sup> O Projeto de Lei nº 2338/2023 institui um marco regulatório nacional para a governança de sistemas de inteligência artificial (IA) no Brasil. O objetivo central da proposição é conciliar o fomento à inovação tecnológica com a proteção de direitos fundamentais e a mitigação de riscos. Para tanto, o projeto estabelece normas gerais que visam garantir a segurança, a confiabilidade e o uso ético e responsável da IA, fundamentado na centralidade da pessoa humana, na transparência e no respeito a valores democráticos. BRASIL. O Projeto de Lei nº 2338/2023. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>. Acesso em: 12 maio 2025.

específico e na classificação de sistemas por nível de risco, com atenção especial aos sistemas generativos como *chatbots*.<sup>118</sup>

Além de definir conceitos-chave para o ecossistema jurídico da IA, o PL 21/2020 propõe princípios fundamentais e introduz o conceito de conhecimento em IA, abrangendo dados, algoritmos, boas práticas e recursos necessários para garantir sua governança:

Art. 1º Esta Lei estabelece princípios, direitos, deveres e instrumentos de governança para o uso da inteligência artificial no Brasil e determina as diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios, pessoas físicas e jurídicas, de direito público ou privado, e entes sem personalidade jurídica em relação à matéria. Art. 2º Para os fins desta Lei, considera-se: I - sistema de inteligência artificial: o sistema baseado em processo computacional que pode, para um determinado conjunto de objetivos definidos pelo homem, fazer previsões e recomendações ou tomar decisões que influenciam ambientes reais ou virtuais; II - ciclo de vida do sistema de inteligência artificial: composto pelas fases, sequenciais ou não, de planejamento e design, coleta e processamento de dados e construção de modelo; de verificação e validação; de implantação; e de operação e monitoramento; III - conhecimento em inteligência artificial: habilidades e recursos, como dados, códigos, algoritmos, pesquisas, programas de treinamento, governança e melhores práticas, necessários para conceber, gerir, entender e participar do ciclo de vida do sistema (Brasil, 2020).

Já o PL 2338/2023, conhecido como Marco Legal da IA, amplia esse escopo ao propor uma regulação mais detalhada, composta por 45 artigos. Seu objetivo é assegurar que o desenvolvimento e uso da IA no Brasil ocorram de forma ética, segura e alinhada à proteção de direitos individuais, à estabilidade democrática e ao progresso tecnológico. No entanto, uma análise preliminar da Autoridade Nacional de Proteção de Dados (ANPD) advertiu que a criação de uma nova entidade reguladora poderia gerar sobreposição de competências, recomendando que a própria ANPD assuma essa governança (Bueno; Santos, 2024, p.118).

Essas propostas legislativas refletem a complexidade multidimensional da regulação da inteligência artificial, que vai muito além da codificação técnica. Envolve o enfrentamento de questões sensíveis como a proteção de dados pessoais, mitigação de vieses algorítmicos e definição de parâmetros claros para a responsabilidade civil por decisões automatizadas. Diante disso, torna-se essencial a construção de um marco regulatório que articule inovação e segurança jurídica com sensibilidade ética e institucional.

---

<sup>118</sup> Adamopoulou e Moussiades (2020) descrevem que *Chatbots* são programas de inteligência artificial que simulam conversas humanas, utilizando Processamento de Linguagem Natural (PLN) e análise de sentimentos. Definidos como agentes de software, eles automatizam diálogos e atuam como um ponto de interação humano-computador. Suas aplicações são vastas, abrangendo desde a educação e o comércio eletrônico até a saúde e o entretenimento. A principal motivação para seu uso é o aumento da produtividade, além de proporcionarem redução de custos operacionais e capacidade de atendimento simultâneo a múltiplos usuários, oferecendo uma interação mais direta e eficiente que as tradicionais FAQs. ADAMOPOULOU, Eleni; MOUSSIADES, Lefteris. Chatbots: História, tecnologia e aplicações. *Aprendizado de Máquina com Aplicações*, v. 2, p. 100006, 2020.

O PL 2338/2023, em particular, destaca-se por incorporar em seus artigos 1º e 2º princípios estruturantes, como a centralidade da pessoa humana, o respeito aos direitos trabalhistas e o desenvolvimento sustentável, refletindo a ampla gama de impactos sociais que a regulação da IA deve considerar:

Art. 1º Esta Lei estabelece normas gerais de caráter nacional para o desenvolvimento, implementação e uso responsável de sistemas de inteligência artificial (IA) no Brasil, com o objetivo de proteger os direitos fundamentais e garantir a implementação de sistemas seguros e confiáveis, em benefício da pessoa humana, do regime democrático e do desenvolvimento científico e tecnológico. Art. 2º O desenvolvimento, a implementação e o uso de sistemas de inteligência artificial no Brasil têm como fundamentos: I – a centralidade da pessoa humana; II – o respeito aos direitos humanos e aos valores democráticos; III – o livre desenvolvimento da personalidade; IV – a proteção ao meio ambiente e o desenvolvimento sustentável; V – a igualdade, a não discriminação, a pluralidade e o respeito aos direitos trabalhistas; VI – o desenvolvimento tecnológico e a inovação; VII – a livre iniciativa, a livre concorrência e a defesa do consumidor; VIII – a privacidade, a proteção de dados e a autodeterminação informativa; IX – a promoção da pesquisa e do desenvolvimento com a finalidade de estimular a inovação nos setores produtivos e no poder público; e X – o acesso à informação e à educação, e a conscientização sobre os sistemas de inteligência artificial e suas aplicações (Brasil, 2023).

Enquanto a proposta legislativa busca consolidar um marco geral, órgãos reguladores setoriais já vêm se antecipando à regulamentação nacional. A Agência Nacional de Vigilância Sanitária (Anvisa)<sup>119</sup>, por exemplo, desenvolve normas específicas para validação de algoritmos voltados ao diagnóstico médico, e o Banco Central tem emitido diretrizes sobre aplicações financeiras de IA, com foco em explicabilidade algorítmica e na prevenção de discriminação automatizada. Essas iniciativas, embora parciais, revelam uma movimentação institucional que antecipa aspectos que provavelmente serão incorporados à futura legislação geral.

Complementando esse panorama normativo, o PBIA, lançado em 2024, articula uma estratégia nacional para o desenvolvimento ético e inclusivo da IA. Seus eixos incluem o incentivo à pesquisa responsável, o estímulo a parcerias público-privadas e a adoção de padrões éticos no setor público, com destaque para sistemas de atendimento automatizado e triagem, como *chatbots* na saúde e serviços públicos digitais:

---

<sup>119</sup> No ano de 2021, a Anvisa organizou um debate focado na ética e na Inteligência Artificial, especificamente no âmbito da saúde. O propósito deste evento foi deliberar sobre os desafios e as oportunidades que emergem do emprego da IA neste setor. Anvisa, 18 out. 2021. BRASIL. Agência Nacional de Vigilância Sanitária (Anvisa). Anvisa adota estratégia baseada em inteligência artificial para otimizar análise de medicamentos. 2024. Disponível em: <https://www.gov.br/anvisa/pt-br/assuntos/noticias-anvisa/2024/anvisa-adota-estrategia-baseada-em-inteligencia-artificial-para-otimizar-analise-de-medicamentos>. Acesso em: 23 maio 2025. BRASIL. Agência Nacional de Vigilância Sanitária (Anvisa). Disponível em: <https://www.gov.br/anvisa/ptbr/assuntos/noticias-anvisa/2024/anvisa-promove-debate-sobre-etica-e-inteligencia-artificial>. Acesso em: 23 maio 2025. Anvisa adota estratégia baseada em inteligência artificial para otimizar análise de medicamentos.

Incentivar pesquisa em IA responsável, com foco em inclusão digital e redução de desigualdades. Promover parcerias entre universidades, empresas e governo para desenvolvimento de soluções em áreas como saúde e agricultura. Estabelecer padrões para uso de IA no serviço público, como *chatbots* de atendimento e sistemas de triagem (Ministério da Ciência e Tecnologia, 2024).

No entanto, a rápida evolução de tecnologias emergentes como *deepfakes*<sup>120</sup> e a harmonização com padrões internacionais exigirão constante atualização do marco normativo. Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) exerce papel estratégico ao garantir que o uso de dados pessoais em sistemas de IA respeite os princípios da LGPD, especialmente os relacionados à finalidade, necessidade, transparência e consentimento. A atuação da ANPD será decisiva para harmonizar inovação tecnológica com a proteção de direitos fundamentais.<sup>121</sup>

Para Castells e Cardoso, a sociedade em rede vai além da mídia tradicional e não cumpre integralmente a promessa libertária da internet: ela opera em uma dualidade entre o controle de grandes conglomerados multimídia sobre o hipertexto digital e a emergência de redes horizontais de comunicação local-global. Essa dinâmica, segundo os autores, molda uma nova cultura digital, onde “na sociedade em rede, a virtualidade é a refundação da realidade através de novas formas de comunicação socializável”<sup>122</sup> (Castells; Cardoso, 2005, p.24).

Ao desafiar consensos estabelecidos, a presente pesquisa demonstra que a tensão entre protecionismo industrial e inovação aberta moldou decisivamente o atraso regulatório brasileiro em IA. Essa análise contraria a tese da agilidade normativa inerente aos marcos setoriais, revelando pelo caso brasileiro a insuficiência de modelos lineares de regulação tecnológica.

---

<sup>120</sup> *Deepfakes* (literalmente, ‘profundamente falsos’), são mídias (vídeos, áudios ou imagens) hiper-realistas criadas por inteligência artificial (IA) que substituem ou sintetiza rostos, vozes e gestos de pessoas reais. Diferentemente de edições tradicionais (como colagem ou dublagem), elas são geradas por algoritmos de aprendizado profundo (*deep learning*), que analisam milhares de imagens e vídeos para reproduzir expressões faciais, movimentos corporais e até padrões vocais com precisão assustadora. BEIGUELMAN, Giselle. As verdades dos deepfakes. Revista Zum, v. 18, pág. 50-58, 2020.

<sup>121</sup> A análise da interação da Inteligência Artificial com o arcabouço legal existente, com destaque para a Lei nº 13.709/2018 (LGPD), constitui um ponto fundamental de investigação. Dada a abrangência da Inteligência Artificial e seu potencial impacto em diversos campos do Direito (consumerista, concorrencial, trabalhista, processual, entre outros), e considerando que sua operacionalização se baseia no tratamento massivo de dados (big data), torna-se essencial que os princípios e valores da proteção de dados estabelecidos pela LGPD sejam considerados e alinhados aos princípios da IA, orientando sua aquisição, desenvolvimento e utilização. MIGUEL, Henrique. Tecnologia da Informação: Legislação Brasileira - Atualização. Brasília: Ministério da Ciência, Tecnologia e Inovações (MCTI), 2024.

<sup>122</sup> CASTELLS, Manuel; CARDOSO, Gustavo. A sociedade em rede: do conhecimento à ação política. 2005. In: Conferência promovida pelo Presidente da República. 2015.

Ora, o caminho para uma regulação madura da IA no Brasil ainda é incipiente, mas os movimentos recentes indicam uma abordagem cautelosa que busca, simultaneamente, não inibir a inovação e proteger direitos fundamentais, acompanhando a evolução tecnológica sem perder de vista os valores democráticos e sociais.

Embora em fase inicial, o Brasil demonstra esforços para conciliar inovação tecnológica com a proteção de direitos fundamentais. Os projetos de lei aqui mencionados buscam sistematizar princípios éticos e mecanismos de governança, focando na transparência e não discriminação. Órgãos setoriais, como Anvisa e Banco Central, regulam áreas críticas, antecipando diretrizes, enquanto o Plano Brasileiro de Inteligência Artificial e a integração com a LGPD reforçam a necessidade de alinhar o uso de dados pessoais a padrões éticos.

Contudo, como alertam Bueno e Santos (2024, p. 131), a ausência de regulação adequada expõe o país a riscos jurídicos imediatos, como o uso de *deepfakes* para fraudes e a reprodução de vieses algorítmicos que perpetuam desigualdades. Esses riscos reforçam a necessidade urgente de leis específicas que garantam um desenvolvimento justo e seguro da IA, prevenindo impactos negativos antes que se agravem.

Essa lacuna regulatória, no entanto, não resulta apenas de inércia legislativa. Para Júnior e Oliveira (2022, p. 107), ela expressa a chamada “crise da lei”, marcada por uma dupla disfunção: a crise de legitimidade (com normas dissociadas da justiça social) e a hiperinflação legislativa (excesso de leis pouco eficazes). Nesse cenário, a Ciência da Legislação emerge como um instrumento metodológico necessário para qualificar a produção normativa, evitando a simples importação de modelos estrangeiros sem adaptação ao contexto brasileiro.<sup>123</sup>

A proposta dos autores baseia-se em dois eixos: a legística material, que orienta o processo normativo desde a definição do problema até a avaliação de impactos; e a técnica legislativa, que exige precisão terminológica e linguagem acessível, especialmente relevante em temas interdisciplinares como responsabilidade civil e viés algorítmico. Além disso, princípios como proporcionalidade e subsidiariedade devem nortear o marco legal, garantindo equilíbrio entre inovação e proteção, com avaliações *ex ante* que antecipem a eficácia e efetividade das normas (Júnior; Oliveira, 2022, p. 110).

Diante desse panorama, torna-se evidente que a regulação estatal da IA é urgente e indispensável para promover inovação segura e ética. O PL 2338/2023 exemplifica essa necessidade, ao prever supervisão humana, responsabilidade civil e governança compartilhada.

---

<sup>123</sup> JÚNIOR, José Eustáquio de Melo; OLIVEIRA, Gustavo Paschoal Teixeira de Castro. Contributos da Legística para a elaboração do marco legal da inteligência artificial no Brasil. *Revista de Informação Legislativa*, v. 60, n. 237, p. 99-114, 2023.

Para Bueno e Santos (2024, p. 136), a atuação do Estado continua sendo o mecanismo mais adequado para assegurar justiça, igualdade e coerência normativa, por meio da imposição de diretrizes uniformes e instrumentos de fiscalização eficazes.

## 5.7 Plataformas Digitais

À medida que a investigação sobre a evolução das normas do direito digital brasileiro avança, torna-se necessário examinar o estado da arte do debate sobre a regulação das plataformas digitais.

Pois bem, a ascensão das plataformas digitais transformou profundamente o ecossistema informacional brasileiro, criando um paradoxo contemporâneo: ao mesmo tempo que democratizam o acesso à informação, essas ferramentas tornaram-se vetores de desinformação em escala sem precedentes. Afinal, a mediação digital transforma a percepção de realidade e, com isso, desafia os paradigmas legais clássicos, especialmente em temas como liberdade de expressão e *fake news*.

Essa ambivalência decorre do fato de que a mediação digital altera profundamente a percepção da realidade, desafiando os paradigmas jurídicos clássicos, especialmente em temas sensíveis como liberdade de expressão e *fake news*. Como explica Castells (1999, p. 462), a comunicação é, por natureza, simbólica e, no ambiente digital, ela reconfigura os sentidos de espaço, tempo e realidade. A integração de temporalidades e a dissolução das fronteiras físicas criam um regime simbólico, no qual o real e o virtual se imbricam, desestabilizando emissores tradicionais e consolidando uma realidade mediada por constructos digitais.

Essa nova ontologia informacional amplia o papel da internet: ela deixa de ser apenas um meio de conexão para se tornar um dispositivo de construção do real. As plataformas digitais, nesse circunstância, encarnam uma contradição constitutiva: são, simultaneamente, ferramentas de emancipação informacional e infraestruturas propensas à dissimulação e à manipulação de dados.

Para Moreira e Moreira Júnior (2023, p. 133) a proliferação de desinformação nas plataformas digitais impõe desafios substantivos às democracias contemporâneas, especialmente no que tange à preservação da soberania informacional e à integridade do debate público. A dinâmica acelerada de compartilhamento, muitas vezes impulsionada por agentes anônimos ou desavisados, dificulta a responsabilização jurídica e enfraquece os mecanismos

tradicionais de controle estatal. Esse cenário se agrava em períodos eleitorais, quando a manipulação informacional interfere diretamente na formação da vontade popular.<sup>124</sup>

Essa dualidade é evidenciada por Neto (2018, p. 71), ao apontar que tais tecnologias podem aprofundar a democracia, como nos casos de portais de transparência ou sistemas de monitoramento da saúde pública, mas também podem concentrar poder nas mãos de quem as controla:

Por um lado, essa tecnologia tem muito a oferecer à democracia, como é o caso dos portais de transparência ou das tecnologias que permitem aprofundar o conhecimento sobre a saúde da população e sua situação econômica. Por outro, essas mesmas ferramentas podem ser utilizadas para aumentar o poder daqueles que controlam as tecnologias. Trata-se, enfim, de uma questão aberta, delicada e tênue, extremamente dependente do contexto em que é feita a análise e da forma como são utilizados esses sistemas.<sup>125</sup>

Essa ambiguidade ganha contornos ainda mais sensíveis quando se trata da regulação das *fake news*, especialmente diante dos dilemas entre liberdade de expressão e controle estatal. No Brasil, a polarização política intensificada durante a pandemia converteu o tema em campo de batalha institucional. Como destacam Figueirêdo e Reis (2022, p. 343), o ativismo judicial do STF, visível em episódios como a CPI da Covid, busca suprir lacunas legislativas em meio a acusações de censura e manipulação discursiva.

Segundo os autores supramencionados, complexa relação entre Executivo, Legislativo e militâncias digitais, judicializa a política. Isso força os tribunais a decidir sobre a estruturação do debate público online e a reinterpretar as leis frente à nova realidade digital:

(...) essa relação intrincada entre o Executivo, o Legislativo e as militâncias virtuais em um contexto marcado pela atividade partidária e divulgação de conteúdos ideológicos desenvolvidas através do recurso à comunicação digital tende a gerar uma espécie de transbordamento da competição política para a arena jurídica, levando as cortes a terem que se pronunciar sobre o modo pelo qual o ordenamento jurídico em vigor pode ser empregado para coibir delitos praticados no ciberespaço, ou mesmo levando os magistrados a promover novos entendimentos a respeito da construção societária proporcionada pela tecnologia de informacional e suas muitas implicações em uma sociedade de fluxos integrados.<sup>126</sup>

<sup>124</sup> MOREIRA, Nelson Camatta; MOREIRA JÚNIOR, Ronaldo Félix. A construção do constitucionalismo digital na era da desinformação: o caso Cambridge Analytica e seu impacto no ecossistema constitucional. *Revista de Informação Legislativa*, 2023.

<sup>125</sup> NETO, Elias Jacob de Menezes et al. Accountability, transparência e assimetria das relações de visibilidade virtuais: análise dos aspectos antidemocráticos das novas tecnologias da informação e comunicação a partir da ideia de filtro bolha. *Revista Direito, Estado e Sociedade*, n. 53, 2018.

<sup>126</sup> Figueirêdo, Simone de Sá Rosa; Reis, Elton Gomes. Poder e norma no ciberespaço. *Revista Thesis Juris*, v. 11, n. 2, p. 325-348, 2022.



No Brasil, o impacto da desinformação digital assumiu contornos dramáticos em eventos recentes como as eleições de 2018 e 2022 e os ataques de 8 de janeiro de 2023, evidenciando a fragilidade do atual marco regulatório frente ao poder das *big techs*<sup>127</sup>. A ausência de normas específicas que responsabilizem adequadamente essas plataformas pela moderação de conteúdos gerou um ambiente onde informações falsas circulam livremente e manipulando a opinião pública.

Para Júnior (2024, p. 77) a digitalização da vida social conferiu às *big techs* um papel central na mediação das interações humanas, impactando diretamente a comunicação, a formação da opinião pública e, por consequência, o funcionamento das democracias. Ao condicionar o exercício da liberdade de expressão e da participação política a estruturas privadas, impõe-se ao direito o desafio de construir marcos regulatórios capazes de assegurar a integridade democrática em um ambiente informacional dominado por lógicas tecnológicas e corporativas.<sup>128</sup>

A transferência do debate público para o ambiente digital ampliou significativamente o poder normativo das *big techs*, cujos códigos e plataformas passaram a regular, de forma privada, dimensões essenciais da vida em sociedade. Ao assumirem o controle sobre a comunicação, os dados pessoais e a infraestrutura digital, essas empresas passaram a exercer funções antes exclusivas do Estado, deslocando o centro das decisões que impactam o espaço público e a cidadania. Diante desse cenário, o direito digital enfrenta o desafio de responder à crescente privatização do poder, formulando mecanismos capazes de preservar a soberania democrática frente à atuação de atores privados que não se submetem ao controle público (Júnior, 2024, p. 80).

Deveras, empresas como Google e Meta atuam como "legisladores privados" e por razões como essa é que surgiu o Projeto de Lei n.º 2630/2020<sup>129</sup> também conhecido como Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. A proposta visa disciplinar a disseminação de desinformação em plataformas digitais e serviços de mensagens

---

<sup>127</sup> *Big Techs* (ou "Grandes Empresas de Tecnologia") é um termo coletivo que designa um grupo de empresas globais de tecnologia altamente dominantes, caracterizadas por seu poder econômico, influência sociocultural e controle sobre mercados digitais. Essas corporações são líderes em inovação, possuem modelos de negócios baseados em plataformas digitais e exercem impacto significativo em setores como comunicação, comércio, entretenimento, finanças e políticas públicas. Exemplos icônicos incluem Google (Alphabet), Apple, Amazon, Meta (Facebook) e Microsoft, embora outras empresas, como Tesla, Netflix e Alibaba, também sejam frequentemente associadas ao termo.

<sup>128</sup> JÚNIOR, Rubens José Kirk de Sanctis. A regulação das big techs no brasil: um imperativo democrático. Revista da Seção Judiciária do Rio de Janeiro, v. 28, n. 60, p. 74-100, 2024.

<sup>129</sup> BRASIL. Projeto de Lei 2630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>. Acesso em: 21 maio 2025.

privadas, estabelecendo parâmetros legais para a atuação dessas empresas no ecossistema informacional.

O PL nº 2.630 propõe um conjunto de medidas que vai desde a responsabilização das plataformas pela propagação de conteúdos falsos e nocivos até a imposição de transparência em algoritmos, conteúdos patrocinados e rastreamento de *bots*<sup>130</sup>. Embora preserve o princípio da liberdade de expressão, o projeto prevê sanções progressivas (chegando a até 10% do faturamento) em caso de descumprimento, além de incluir ações educativas e a tipificação de crimes eleitorais relacionados à desinformação.

O texto, no entanto, não está isento de controvérsias. Entre os pontos mais debatidos estão a remuneração obrigatória de conteúdos jornalísticos, defendida por veículos de imprensa como mecanismo de justiça econômica, mas criticada por alguns setores por potencialmente beneficiar fontes de desinformação. Outra polêmica é a imunidade parlamentar para conteúdos publicados nas plataformas, medida que poderia fragilizar os instrumentos de combate à desinformação de cunho político<sup>131</sup> (D'almonde; Santos, 2024, p.11).

De forma mais ampla, o legislativo brasileiro tem buscado responder a esses desafios com propostas como o PL 2.630/2020<sup>132</sup>, conhecido como Lei das Fake News, e o PL 2.768/2022<sup>133</sup> sobre inteligência artificial. Esses projetos tentam estabelecer um equilíbrio delicado entre liberdade de expressão e responsabilidade digital, impondo obrigações de transparência e mecanismos de supervisão às plataformas.

---

<sup>130</sup> *Bot* (abreviação de "robot", do inglês "robô") é um *software* autônomo programado para executar tarefas automatizadas, repetitivas e pré-definidas, geralmente em ambientes digitais. Sua função principal é simular ações humanas em sistemas computacionais, operando de forma autônoma ou semiautônoma, com base em algoritmos, regras pré-estabelecidas ou modelos de inteligência artificial (IA).

<sup>131</sup> D'ALMONTE, Edson Fernando; SANTOS, Alanna Oliveira. Regulamentação das plataformas digitais: entre a soberania digital e o transnacionalismo. In: E-Compós. 2024.

<sup>132</sup> BRASIL. Projeto de Lei 2.630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. O PL constitui um marco normativo em elaboração que busca regular as atividades de provedores de redes sociais e serviços de mensageria privada no Brasil. Sua finalidade abrange a promoção da segurança e liberdade de expressão online, bem como o combate a práticas consideradas prejudiciais ao ambiente digital e ao processo democrático, mediante a imposição de obrigações de transparência, responsabilidade e moderação, além da criação de instâncias de acompanhamento e aplicação de sanções. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>. Acesso em: 12 maio 2025.

<sup>133</sup> O PL disciplina a regulação de plataformas digitais no Brasil, estabelecendo marco legal para atuação, fiscalização e sanção. Atribui à ANATEL competência central para normatização, supervisão e penalidades a operadores com poder de controle de acesso essencial (definido por receita operacional), objetivando concorrência, acesso à informação, inovação e proteção de usuários, com observância à livre iniciativa e defesa do consumidor. Prevê o FisDigi para financiar fiscalização e fomento à inovação digital, sob regime sancionatório gradativo, preservando as competências do CADE em matéria concorrencial. BRASIL. Projeto de Lei 2.768/2022. Dispõe sobre a organização, o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro e dá outras providências.

No entanto, esses projetos enfrentam forte resistência das próprias empresas de tecnologia, que argumentam que tais medidas ameaçam a liberdade na internet. Ao mesmo tempo, esses atores mantêm modelos de negócios centrados na coleta massiva de dados e no engajamento Estado de regular atividades online dentro de seu território frente ao poder transnacional e assimétrico das *big techs*.

A questão da jurisdição sobre plataformas digitais tornou-se particularmente crítica em episódios como o bloqueio judicial do Telegram em 2022<sup>134</sup>, quando a empresa resistiu a cumprir determinações da Justiça brasileira. Situações como essa evidenciam a limitação do atual arcabouço jurídico nacional, ainda que pautado por marcos importantes como o MCI e a LGPD. Ambos, embora inovadores em seu tempo, têm se mostrado insuficientes para enfrentar os desafios impostos por uma economia digital cada vez mais globalizada e assimétrica.

Enquanto o MCI consagra princípios fundamentais como a neutralidade da rede, ele avança pouco na regulação da moderação responsável de conteúdo. Já a LGPD, apesar de representar um marco importante na proteção de dados pessoais, enfrenta entraves operacionais frente à complexidade das estruturas empresariais das *big techs*, que muitas vezes operam fora do alcance efetivo da regulação nacional.

Esse impasse reflete um dilema global contemporâneo: como conciliar inovação tecnológica com proteção democrática, em um contexto em que as fronteiras jurídicas tradicionais são desafiadas pela natureza transnacional da internet. A experiência brasileira recente ilustra que, sem uma regulação clara, assertiva e coordenada, as plataformas digitais tendem a se transformar em arenas de manipulação informacional, impactando de maneira negativa não apenas o debate público, mas os próprios alicerces da democracia representativa.

A essa altura, torna-se evidente que o impacto das redes digitais transcende o campo da comunicação, afetando profundamente a estrutura social, econômica e política. Como aponta Castells (1999, p. 565), as “redes constituem a nova morfologia social de nossas sociedades e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura”. Em outras palavras, as plataformas digitais não são apenas intermediárias técnicas, mas atores estruturantes das dinâmicas de poder e construção simbólica do real.

---

<sup>134</sup> BRASIL. Supremo Tribunal Federal. STF notícias: Ministro Alexandre de Moraes dá prazo para Telegram cumprir integralmente determinações do STF O ministro manteve a decisão que ordenou o bloqueio do aplicativo e afirmou que o cumprimento total é necessário para que seja suspensa a ordem de tirar o Telegram do ar. Petição 9.935 Distrito Federal. Disponível em: <https://noticias.stf.jus.br/postsnoticias/ministro-alexandre-de-moraes-da-prazo-para-telegram-cumprir-integralmente-determinacoes-do-stf/>. Acesso em 30 jun. 2025.

Diante disso, o caminho adiante das plataformas digitais exige a construção de um marco regulatório moderno e responsivo, capaz de promover transparência algorítmica, responsabilização institucional e respeito às instituições democráticas, sem engessar a inovação tecnológica. Trata-se de um desafio complexo e inadiável que o Brasil precisa enfrentar com firmeza jurídica, visão sistêmica e diálogo multissetorial, sob pena de perder sua autonomia regulatória e comprometer o futuro de sua cidadania digital.

## 6 O DIREITO DIGITAL À LUZ DA CONSTITUIÇÃO

O Direito Digital não deve ser visto como algo totalmente novo. Na verdade, ele se apoia fortemente nos princípios já consolidados do Direito e faz amplo uso da legislação vigente. O que realmente muda é a maneira como essas normas são interpretadas e aplicadas diante das novas demandas tecnológicas. Assim, é incorreto imaginar que a tecnologia gera um vazio legal em que a sociedade estaria desprotegida, pois as normas vigentes continuam sendo válidas para essas situações, desde que interpretadas adequadamente. Essa área do Direito representa a continuidade evolutiva do ordenamento jurídico, respeitando os fundamentos constitucionais que sustentam o Estado Democrático de Direito (Pinheiro, 2021, p. 53).

Trata-se de uma ampliação dos institutos tradicionais, aplicando-os a novas realidades digitais, sem perder de vista os direitos e garantias fundamentais estabelecidos pela Constituição:

O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.) (Pinheiro, 2021, p. 49).

A regulação das atividades econômicas no ambiente digital encontra seu fundamento constitucional no artigo 170 da Constituição Federal, que estrutura a ordem econômica brasileira sobre os pilares da valorização do trabalho humano e da livre iniciativa. Nessa perspectiva, a jurisprudência do STF<sup>135</sup> tem revelado uma tensão recorrente entre a liberdade econômica e a necessidade de intervenção estatal para proteger outros princípios constitucionais, como a defesa do consumidor, a proteção ambiental (inclusive do ciberespaço), a livre concorrência e os direitos trabalhistas.

---

<sup>135</sup> Para ilustrar, colaciona-se ADI 6.921/6.931: “Medida Provisória 1018/2020. Conversão na Lei 14.173/2021. Emenda parlamentar. Inclusão do art. 32, §15, da Lei 12.485/2011. Carregamento de canais de programação de distribuição obrigatória por distribuidoras de tv por assinatura (must-carry). (...) O princípio da livre iniciativa, garantido no art. 170 da Constituição, não proíbe o Estado de atuar subsidiariamente sobre a dinâmica econômica para garantir o alcance de objetivos indispensáveis para a manutenção da coesão social, entre eles a proteção do consumidor e a redução das desigualdades regionais e sociais (art. 170, V e VII, da CF), bem como a promoção da cultura nacional e regional e a regionalização da produção cultural, artística e jornalística (art. 221, II e III, da CF), desde que haja proporcionalidade entre a restrição imposta e a finalidade de interesse público, o que ocorre no caso. (ADI 6.921 e ADI 6.931, rel. min. Alexandre de Moraes, j. 07.02.2024, P, DJE de 03.05.2024)”. BRASIL. Supremo Tribunal Federal. A Constituição e o Supremo. Anotações do Supremo Tribunal Federal. Disponível em: <https://constituicao.stf.jus.br/dispositivo/cf-88-parte-1-titulo-7-capitulo-1-artigo-170>. Acesso em 20 maio 2025.

Essa tensão normativa se amplia quando se considera a dimensão tecnológica da atividade econômica. A Constituição de 1988, por meio dos Artigos 218 e 219, impõe ao Estado o dever de fomentar o desenvolvimento científico e tecnológico, como forma de impulsionar o progresso nacional. Esse compromisso foi reforçado com a promulgação da Emenda Constitucional nº 85/2015<sup>136</sup> que atualizou tais dispositivos e consagrou a priorização da pesquisa científica (básica e aplicada) orientada à solução de problemas nacionais e ao fortalecimento da capacidade produtiva.<sup>137</sup>

A EC nº 85/2015 representou, portanto, um marco jurídico relevante ao incorporar ao texto constitucional a noção de que o avanço tecnológico requer cooperação estruturada entre universidades, centros de pesquisa e setor produtivo. Essa mudança não se deu por acaso: foi resultado da mobilização da comunidade científica e tecnológica (C&T), que pleiteava condições institucionais mais robustas para viabilizar a autonomia tecnológica brasileira. Além de atualizar os artigos 218 e 219, a emenda também reforçou o papel estratégico da parceria público-privada no ecossistema de inovação nacional (Bucci, 2017, p. 314).<sup>138</sup>

Nesse mesmo sentido, a Constituição de 1988 inovou ao dedicar um capítulo à C&T<sup>139</sup>, reconhecendo sua importância para o desenvolvimento socioeconômico. Embora o artigo 218<sup>140</sup> possua redação genérica, ele orienta a formulação de políticas públicas ao estabelecer

<sup>136</sup> BRASIL. Emenda constitucional nº 85, de 26 de fevereiro de 2015. Altera e adiciona dispositivos na Constituição Federal para atualizar o tratamento das atividades de ciência, tecnologia e inovação. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/Emendas/Emc/emc85.htm#art1](https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc85.htm#art1). Acesso em 20 maio 2025.

<sup>137</sup> Os artigos constitucionais 218, 219, 219-A e 219-B são a base jurídica da política brasileira de ciência, tecnologia e inovação, e estruturam a análise da evolução do Direito Digital feita na dissertação. O Art. 218 estabelece o compromisso do Estado com o desenvolvimento científico e tecnológico, justificando políticas como a reserva de mercado em informática, incentivos à pesquisa (como os da Lei nº 8.248/1991) e a priorização de soluções para demandas nacionais, refletidas em marcos como a LGPD e o Marco Civil da Internet. O Art. 219 reforça a defesa do mercado interno e da autonomia tecnológica, fundamentos para regulações estratégicas como a proteção de dados e segurança cibernética. Já os Arts. 219-A e 219-B destacam a importância da cooperação público-privada e da criação do SNCTI, fundamentais para a governança digital e temas como interoperabilidade e plataformas digitais. BRASIL. Constituição da República Federativa do Brasil de 1988: promulgada em 5 de outubro de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 20 maio 2025.

<sup>138</sup> BUCCI, Maria Paula Dallari; COUTINHO, Diogo R. Arranjos jurídico-institucionais da política de inovação tecnológica: uma análise baseada na abordagem de direito e políticas públicas. Inovação no Brasil: avanços e desafios jurídicos e institucionais. São Paulo: Blucher, p. 313-340, 2017.

<sup>139</sup> “O termo ‘ciência’, enquanto atividade individual, faz parte do catálogo dos direitos fundamentais da pessoa humana (inciso IX do art. 5º da CF). Liberdade de expressão que se afigura como clássico direito constitucional-civil ou genuíno direito de personalidade. Por isso que exigente do máximo de proteção jurídica, até como signo de vida coletiva civilizada. Tão qualificadora do indivíduo e da sociedade é essa vocação para os mistérios da Ciência que o Magno Texto Federal abre todo um autonomizado capítulo para prestigiá-la por modo superlativo (Capítulo de n. IV do Título VIII).

<sup>140</sup> A regra de que “o Estado promoverá e incentivará o desenvolvimento científico, a pesquisa e a capacitação tecnológicas” (art. 218, caput) é de logo complementada com o preceito (§ 1º do mesmo art. 218) que autoriza a edição de normas como a constante do art. 5º da Lei de Biossegurança. A compatibilização da liberdade de expressão científica com os deveres estatais de propulsão das ciências que sirvam à melhoria das condições de vida para todos os indivíduos. Assegurada, sempre, a dignidade da pessoa humana, a CF dota o bloco normativo

diretrizes como o financiamento prioritário à pesquisa básica, especialmente aquela voltada ao interesse público e ao avanço científico. Essa priorização, no entanto, enfrenta limitações operacionais, como a escassez de recursos e a ausência de critérios normativos objetivos para hierarquizar linhas de pesquisa, o que compromete a efetividade da política científica nacional (Tavares, 2007, p. 9).<sup>141</sup>

Diretrizes explícitas, como o apoio à formação de recursos humanos e o incentivo a investimentos privados em Pesquisa, Desenvolvimento e Inovação (P&D+I), ganharam força com a promulgação da Emenda Constitucional nº 85/2015. Essa emenda representou um avanço importante ao estimular a colaboração entre o setor público e o privado, promover a internacionalização da ciência brasileira e incentivar a formação de um mercado interno robusto e competitivo, elementos essenciais para a construção de um ecossistema digital inovador e governável.

Esse reforço às políticas de fomento encontra sustentação no arcabouço constitucional mais amplo, que inclui o Sistema Nacional de Ciência, Tecnologia e Inovação (SNCTI) e o princípio da competência legislativa concorrente, o que garante coerência federativa no alinhamento entre desenvolvimento tecnológico e objetivos nacionais estratégicos.

No plano interpretativo, a jurisprudência do STF também tem contribuído para consolidar esse entendimento. Em decisões como a ADI 3.510<sup>142</sup>, a Corte reconhece a liberdade de pesquisa científica como direito fundamental (artigo 5º, IX da CF/88), bem como o dever do Estado de fomentá-la (artigo 218). Esse binômio é balizado pela necessidade de respeito à dignidade da pessoa humana, estabelecendo os contornos éticos para o uso de tecnologias disruptivas:

O termo ‘ciência’, enquanto atividade individual, integra o catálogo de direitos fundamentais (Art. 5º, IX da CF/88). A obrigação estatal de promover o desenvolvimento científico (Art. 218) é complementada pelo § 1º do mesmo artigo, que autoriza normas como o Art. 5º da Lei de Biossegurança, desde que respeitada a dignidade da pessoa humana. (Brasil, STF, ADI 3.510, Rel. Min. Ayres Britto, j. 29.05.2008).

---

posto no art. 5º da Lei 11.105/2005 do necessário fundamento para dele afastar qualquer invalidade jurídica (ministra Cármen Lúcia). (ADI 3.510, rel. min. Ayres Britto, j. 29-5-2008, P, DJE de 28-5-2010.)

<sup>141</sup> TAVARES, André Ramos. Ciência e tecnologia na Constituição. Revista de Informação Legislativa. Brasília: Senado Federal, a, v. 44, p. 7, 2007.

<sup>142</sup> BRASIL. Supremo Tribunal Federal (Plenário). Ação Direta de Inconstitucionalidade 3.510/DF. Relator: Min. Ayres Britto, 29 maio 2008. Diário de Justiça Eletrônico, Brasília, DF, 28 maio 2010. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjurl78396/false>. Acesso em: 22 abr. 2025.

A evolução normativa histórica refletiu na constitucionalização da proteção digital, que posteriormente culminou em marcos específicos para o ambiente digital, destacando-se a LGPD, que estabeleceu um regime jurídico para o tratamento de dados pessoais por entes públicos e privados, detalhando regras sobre coleta, uso, armazenamento e compartilhamento, com o objetivo de proteger a privacidade e garantir transparência e responsabilidade. Bem como introduziu princípios basilares, como a finalidade específica e legítima para o tratamento, e um rol de direitos aos titulares (acesso, retificação, exclusão etc.), reforçando a autodeterminação informativa.<sup>143</sup>

Mais do que uma norma técnica, a LGPD representa a tentativa do legislador de equilibrar o dinamismo econômico e tecnológico com a proteção da esfera informacional do indivíduo. Ao introduzir princípios como finalidade específica, legitimidade no tratamento e direitos dos titulares (como acesso, retificação e exclusão), a lei busca consolidar uma nova gramática jurídica para o ecossistema digital.

Nesse novo arranjo, a proteção de dados pessoais assume dupla dimensão: de um lado, como direito fundamental e, de outro, como elemento estratégico para a competitividade econômica, ao garantir confiança institucional e equidade no ambiente digital.

Logo, a convergência entre os dispositivos constitucionais sobre ordem econômica, ciência e tecnologia e direitos fundamentais forma o núcleo estruturante da regulação da economia digital no Brasil. Essa arquitetura jurídico-constitucional impõe ao Estado o dever de atuar como mediador qualificado entre inovação e proteção, assegurando que o avanço tecnológico ocorra dentro de parâmetros éticos, democráticos e socialmente responsáveis.

## **6.1 A centralidade dos princípios na regulação digital**

Nesta etapa da pesquisa, torna-se pertinente questionar se a abordagem regulatória atualmente adotada pelo Brasil em matéria de Direito Digital é, de fato, a mais adequada para assegurar a atualização constante das normas jurídicas diante da velocidade exponencial das

---

<sup>143</sup> Para Grossi (2020, p. 22), a autodeterminação Informativa se trata do direito inerente ao indivíduo de exercer controle e assegurar a proteção de seus dados pessoais, notadamente diante da evolução tecnológica e dos procedimentos de tratamento da informação. Observa-se que tal direito constitui uma especificação do direito à privacidade, na qual se exige que o indivíduo detenha a capacitação e o conhecimento necessários para deliberar livremente sobre as operações de tratamento que recaem sobre seus dados. A análise revela que o controle individual sobre o trânsito dos dados do próprio titular configura uma extensão das liberdades individuais, integrando simultaneamente as abordagens da privacidade de dados de natureza negativa e estática com a perspectiva dinâmica e protetiva que acompanha o percurso integral dos dados nos diversos meios de circulação. GROSSI, Bernardo Menicucci. Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico]. Porto Alegre, RS: Editora Fi, 2020.



transformações tecnológicas. Afinal, uma vez consolidada determinada norma, será possível mantê-la efetiva e compatível com as inovações emergentes? Com isso em mente, propõe-se, doravante, uma análise crítica da forma como o ordenamento jurídico brasileiro tem enfrentado os desafios estruturais da regulação digital.

Nessa realidade, evidencia-se um descompasso ontológico no modelo vigente: a tentativa de normatizar, por meio da legislação, tecnologias em permanente aceleração colide com a obsolescência precoce das regras jurídicas. Essa tensão revela uma assimetria sistêmica entre o tempo do Direito e o tempo da tecnologia, expondo a insuficiência de modelos normativos excessivamente casuísticos ou engessados.

Diante dessa assimetria, impõe-se a primazia de princípios gerais (flexíveis e adaptativos) sobre regras casuísticas. Questiona-se, assim, se o modelo fragmentário vigente, materializado em estatutos setoriais como a LGPD e o MCI, assegura efetividade regulatória diante da dinâmica disruptiva do ecossistema digital, ou se consolida uma ficção de segurança jurídica desconectada da realidade tecnossocial.

Nesse contexto, propostas legislativas como o PL 2.630/2022 (também conhecido como Lei das *Fake News*) ilustram com clareza a crise regulatória contemporânea. Seu processo de tramitação legislativa escancara tensões não resolvidas entre o exercício do controle estatal e a proteção da liberdade de expressão, além de evidenciar a inadequação dos instrumentos normativos tradicionais frente ao poder transnacional das *big techs* e à reconfiguração algorítmica do espaço público digital.

Importa destacar que essa defasagem entre Direito e tecnologia não é inédita, mas se intensifica dramaticamente na era digital, assumindo proporções inéditas. Ela levanta questões cruciais sobre a eficácia da abordagem regulatória atual e sobre a real capacidade do Direito de garantir direitos fundamentais sem inibir a inovação tecnológica, um equilíbrio cada vez mais complexo e estratégico na consolidação de uma sociedade digital democrática<sup>144</sup>:

(...) ocorre a apropriação do espaço digital pelo poder privado, o que amplia, ainda mais, a coleta, armazenamento e processamento de dados em larga escala (*big data*). Essa situação, conforme será visto neste artigo, atinge, especificamente, a democracia, que necessita de visibilidade e de *accountability*, elementos que não são encontrados no atual cenário de uso privado das tecnologias da informação (Neto et. al, 2018, p. 63).

---

<sup>144</sup> NETO, Elias Jacob de Menezes et al. *Accountability, transparência e assimetria das relações de visibilidade virtuais: análise dos aspectos antidemocráticos das novas tecnologias da informação e comunicação a partir da ideia de filtro bolha*. Revista Direito, Estado e Sociedade, n. 53, 2018.

As plataformas digitais, especialmente as chamadas *big techs*, ascenderam a uma posição de domínio sem precedentes, reconfigurando profundamente as relações sociais, econômicas e políticas em escala global. Com modelos de negócios baseados na extração massiva de dados e na lógica algorítmica, essas empresas passaram a operar como verdadeiras infraestruturas cívicas, exercendo influência direta sobre os fluxos de informação, o consumo cultural e até mesmo os processos democráticos.

Diante desse cenário, D’Almonte e Santos (2024) realizaram um estudo revelador sobre a proposta de regulação das plataformas no Brasil, representada pelo Projeto de Lei 2.630/2022. Segundo os autores, o debate público em torno da proposta reflete uma profunda polarização política: enquanto alguns setores o celebram como o “PL das Fake News”, outros o denunciam como o “PL da Censura”. Essa dicotomia, observam, sintetiza a crise contemporânea do espaço público digital e espelha os desafios enfrentados globalmente no esforço de limitação do poder das *big techs*.

Nesse enredo, os autores identificam três modelos regulatórios principais: a autorregulação, promovida pelas próprias plataformas; a regulação coercitiva estatal; e a correção cooperativa, que busca integrar Estado, sociedade civil e setor privado. Ainda assim, um entrave central permanece: o poder oligopolístico dessas corporações, que, ao formar "cartéis de conteúdo", conseguem contornar normas nacionais, colocando em xeque a eficácia dos direitos humanos como freios culturais ao domínio informacional transnacional (D’Almonte; Santos, 2024, p. 4).

A análise dos autores se aprofunda ao revisitar o conceito de espaço público habermasiano, historicamente concebido como uma arena discursiva racional, agora profundamente alterada pelo domínio das plataformas digitais. Essas, que inicialmente se apresentaram como catalisadoras de uma “cultura participativa”, acabaram por se consolidar como infraestruturas algorítmicas, mediando ativamente o acesso à informação e subordinando o discurso público a valores corporativos e interesses comerciais.

Dessa forma, o controle privado dos fluxos comunicacionais por empresas que concentram audiência, infraestrutura e dados gera impactos estruturais na democracia, exigindo um arcabouço regulatório em três eixos, quais sejam: a proteção de dados pessoais, os direitos autorais sobre conteúdo digital e o combate à desinformação intencional. A crescente migração do consumo de notícias para plataformas como TikTok (14% entre jovens brasileiros em 2023) e Instagram, operando sob lógica algorítmica e formação de bolhas ideológicas, fragiliza o debate público plural e compromete os fundamentos deliberativos da democracia (D’Almonte; Santos, 2024, p. 6).

O cerne do dilema regulatório contemporâneo reside na definição da responsabilidade das plataformas digitais na garantia dos direitos humanos, sem comprometer a liberdade de expressão. O cenário atual é marcado por uma zona cinzenta jurídica, onde essas corporações oscilam entre a imunidade de meras hospedeiras e as cobranças crescentes por moderação ativa, revelando não apenas falhas de governança estatal, mas também a crise da soberania digital. Enquanto os Estados Unidos apostam em uma autorregulação ancorada na Primeira Emenda, a União Europeia avança com regulações estatais robustas.

Diante disso, D'Almonte e Santos (2024, p. 8) propõem um modelo de correção baseado em direitos humanos, estruturado em três pilares: (1) atuação estatal para assegurar proporcionalidade na regulação de conteúdo; (2) transparência e compromissos públicos por parte das plataformas; e (3) mecanismos processuais acessíveis para usuários

Essa discussão adquire particular relevância no contexto brasileiro, onde a liberdade de expressão foi consagrada como pilar constitucional após a ditadura, conforme o artigo 5º da CF/88, e reforçada em decisões emblemáticas do STF, como na ADPF 130, que revogou a anacrônica Lei de Imprensa de 1967.

Contudo, como observam Freitas, Lunardi e Correia (2024, p. 9), esse arcabouço jurídico foi concebido para lidar com a mídia tradicional, sem antecipar a emergência do poder censório privado das plataformas digitais. Estas, ao moderar conteúdos com base em algoritmos opacos e práticas como *shadow banning*<sup>145</sup>, passaram a controlar silenciosamente a circulação de ideias, sem supervisão democrática, gerando graves implicações para o Estado de Direito.<sup>146</sup>

O desafio torna-se ainda mais agudo diante da natureza transnacional dessas plataformas e do poder exponencial da inteligência artificial, como apontam Filho e Ladeira (2021, p. 93). Segundo os autores, esse cenário torna as regulações nacionais estruturalmente ineficazes, corroendo a capacidade regulatória dos Estados. Ao passo que EUA e China evitam legislações restritivas por razões estratégicas, a União Europeia tem liderado o caminho com marcos como o Regulamento de Inteligência Artificial (2021), ancorado na proteção dos direitos fundamentais.

---

<sup>145</sup> Método de censura por algoritmos que tem como função limitar, de uma forma preestabelecida, e sem que haja o conhecimento ou consentimento do usuário do aplicativo, a possibilidade de exposição geral de determinada postagem feita na rede social. FREITAS, Luiz Otávio Rezende de; LUNARDI, Fabrício Castagna; CORREIA, Pedro Miguel Alves Ribeiro. Liberdade de expressão na era digital: novos intermediários e censura por atores privados. Revista de Investigações Constitucionais, v. 11, n. 2, p. e262, 2024.

<sup>146</sup> FREITAS, Luiz Otávio Resende de; LUNARDI, Fabrício Castagna; CORREIA, Pedro Miguel Alves Ribeiro. Liberdade de expressão na era digital: novos intermediários e censura por atores privados. Revista de Investigações Constitucionais, Curitiba, vol. 11, n. 2, e262, maio/ago. 2024.

No plano teórico, os autores recorrem à teoria dos sistemas de Luhmann e Teubner para descrever a incomunicabilidade entre os sistemas jurídico e tecnológico, cada qual operando em linguagens autopoieticas. Sob essa perspectiva, a regulação jurídica só se torna efetiva quando normas externas são internalizadas como autorregulação ética pelas plataformas, motivadas por “irritações normativas” (Filho; Ladeira, 2021, p. 93).

Desse modo, os direitos fundamentais assumem dupla função: atuam como freios à hipertrofia tecnológica e como estímulos à autolimitação dos sistemas digitais. A esperança normativa, nesse cenário, repousa na cultura *hacker/geek* (comunidades tecnológicas), descrita por Keltly, que cultiva uma ética de compartilhamento, transparência e solidariedade, servindo como base para uma autorregulação orientada por valores humanos (Filho; Ladeira, 2021, p. 93).<sup>147</sup>

O Direito Digital consolida-se como uma evolução adaptativa do Direito tradicional, abandonando o predomínio de regras rígidas em favor da primazia de princípios, como resposta à aceleração tecnológica<sup>148</sup>. Seu núcleo opera pela autorregulamentação construída pelos atores digitais e aplicação dinâmica de princípios costumeiros (generalidade, uniformidade, continuidade, notoriedade), sustentada por mecanismos ágeis como analogia e arbitragem.

Esta abordagem, refletida no PL 21/2020 (que regula tecnologias emergentes com base em princípios, nos moldes da OCDE), evita a obsolescência normativa e adapta institutos clássicos (contratos, prova digital) à realidade algorítmica, preservando segurança jurídica sem engessar a inovação (Barbosa; Pinheiro, 2023, p. 33).

Entretanto, essa proposta contrasta com a tradição brasileira de produção legislativa setorial, especialmente no pós-1988. Leis como a Lei Carolina Dieckmann e o MCI têm sido criticadas por sua abordagem fragmentada e reativa. O MCI, por exemplo, fragilizou a proteção contra conteúdos lesivos ao substituir a jurisprudência do *notice and take down* (procedimento de remoção de conteúdo). Já a Lei Geral de Proteção de Dados (LGPD), apesar de inovar ao prever direitos explícitos aos titulares, perpetua riscos doutrinários, como a fragmentação interpretativa e a falsa percepção de autossuficiência normativa, obstruindo o necessário

---

<sup>147</sup> FILHO, Marco Aurélio Florêncio; LADEIRA, Fernando. Cidadania digital ou ditadura algorítmica? Contradições do mundo digitalizado e os desafios da regulação. *Duc In Altum-Cadernos de Direito*, v. 13, n. 31, 2021.

<sup>148</sup> Ao ponderar princípios constitucionais (liberdade de expressão, honra, privacidade, legalidade, proporcionalidade e responsabilidade civil), o Supremo deve harmonizá-los com os pilares do Marco Civil da Internet, liberdade de expressão, proteção da privacidade, neutralidade da rede e responsabilidade subjetiva do artigo 19 (exigindo ordem judicial para remoção de conteúdo), e os princípios da LGPD (finalidade, necessidade, segurança, transparência e não discriminação no tratamento de dados). A decisão buscará equilíbrio entre proteção da expressão e prevenção de danos, assegurando uso ético de dados e respeito ao requisito judicial de remoção.

diálogo de fontes. Seu maior déficit, segundo Frazão, Oliva e Tepedino (2020, p. 170), está na distância entre o reconhecimento abstrato de direitos e sua efetividade prática.

Nesse enquadramento, o PL 2.630/2022 surge como tentativa de superação desse vácuo regulatório, com mecanismos que impõem transparência algorítmica, identificação de *bots*, relatórios periódicos, e sanções progressivas. O projeto também fortalece o papel do Comitê Gestor da Internet (CGI). Apesar das críticas, como a potencial ampliação da imunidade parlamentar e as controvérsias sobre remuneração obrigatória a veículos jornalísticos, o projeto representa um avanço estrutural no enfrentamento da lógica *data-driven* (guiada por dados) das plataformas, que monetizam atenção e desinformação em detrimento da saúde do espaço público (D'almonte; Santos, 2024, p. 11-14).

Segundo Pereira e Junior (2024) a ausência de consenso entre juristas e legisladores reflete a incompatibilidade entre a dinâmica das inovações e a natureza estabilizadora do sistema jurídico:

Com efeito, por qualquer perspectiva que se observe, dentre as diversas correntes e marcos teóricos adotados, como exemplificado acima, é possível perceber que o Direito assume um certo papel de perplexidade diante do potente fenômeno das Big Tech. Embora tal perplexidade não signifique uma paralisia, já que se percebe um claro crescimento do interesse dos juristas em enfrentar o desafio maior de nosso tempo, que é o do enfrentamento das questões trazidas pelas novas tecnologias sobre a sociedade. Ainda assim, pode-se afirmar que, ao menos neste momento, não há consenso no que tange ao melhor caminho a ser seguido, ao passo em que a ciência do Direito e mesmo os legisladores ao redor do mundo buscam alcançar o avanço tecnológico e se adequar ao seu apressado ritmo (Pereira; Junior, 2024, p. 8).<sup>149</sup>

A pesquisa de Seto (2021, p. 238) aprofunda essa crítica ao demonstrar que os marcos regulatórios brasileiros possuem falhas estruturais graves, como a incoerência entre compromissos internacionais e normativas internas. Um exemplo é a rejeição, pelo CGI.br, da técnica de *deep packet inspection* (análise de tráfego de rede), considerada violadora da neutralidade da rede, apesar de sua aceitação tácita em acordos internacionais.

Além disso, o MCI falha ao limitar sua aplicação territorial, deixando descobertos dados tratados fora do Brasil, enquanto a LGPD, embora tenha pretensão extraterritorial, enfrenta limitações práticas: fragilidade da ANPD, ausência de medidas coercitivas eficazes, e exclusões normativas problemáticas (como as plataformas financeiras).<sup>150</sup>

<sup>149</sup> PEREIRA, Laurence Duarte Araújo; FALEIROS, José Luiz de Moura Júnior. Regulação das plataformas digitais no Brasil e a defesa da soberania nacional. Revista de Ciências do Estado, Belo Horizonte, v. 9, n. 1, p. 1-22, 2024.

<sup>150</sup> SETO, Kenzo Soares. A regulação e governança das plataformas digitais: uma revisão sistemática de literatura. Revista Eptic Online, v. 23, n. 3, 2021.

A partir dessas análises, evidencia-se que os modelos vigentes de regulação digital enfrentam um impasse ontológico: entre autorregulação transnacional e tentativas de governança híbrida, ambas travadas pela indefinição do que constitui o “interesse público” no ambiente digital. Essa polarização repete-se nos debates sobre *big data*, IA e soberania informacional, onde os marcos normativos revelam-se ainda incapazes de garantir efetiva autonomia e proteção de direitos no fluxo global de dados.

Acende-se um alerta para a crescente fragmentação nas propostas de regulação de algoritmos (sejam elas estatais, híbridas ou independentes) e para o risco de surgimento de mercados privados de regulação, onde grandes corporações definem suas próprias regras de funcionamento. Como alerta Seto (2021, p. 242), a ausência de padrões claros de segurança para serviços críticos e a falta de marcos éticos robustos para tecnologias como a IA e o 5G podem reforçar monopólios digitais e ampliar assimetrias de poder informacional. Nesse contexto, o cenário brasileiro permanece reativo e sem coordenação, agravado pela ausência de um consenso normativo capaz de acompanhar o ritmo dos avanços tecnológicos.

Diante dessa omissão legislativa, especialmente no que tange à responsabilidade civil das plataformas digitais, o STF foi chamado a atuar como protagonista regulador, ocupando o vazio normativo deixado pelo Congresso Nacional. No julgamento de repercussão geral sobre o artigo 19 do Marco Civil da Internet, debateu-se o delicado equilíbrio entre a proteção dos direitos fundamentais e a liberdade de expressão digital.<sup>151</sup>

Nessa perspectiva, para Júnior (2024, p. 94), quanto a diretriz do artigo 19, embora voltada à proteção da liberdade de expressão, tem se mostrado insuficiente diante da crescente complexidade do ecossistema digital:

Estabelecido esse panorama da situação regulatória no Brasil, é possível constatar que o modelo de regulação, precário e insuficiente, previsto no artigo 19 do Marco Civil da Internet, tem sido objeto de uma reformulação legislativa completa. Essa reformulação busca aproximar o Brasil de modelos regulatórios que atribuem às grandes companhias de tecnologia (Big Techs) diversas obrigações na estruturação e no desenho de suas atividades, impondo-lhes deveres de cuidado (ou diligência), transparência e autorregulação, como o fornecimento de relatórios sistêmicos a serem fiscalizados pela sociedade e por autoridades governamentais.

---

<sup>151</sup> Paralelos ao julgamento do STF, os REs 1037396 e 1057258 debatem a responsabilidade civil de plataformas digitais: o primeiro questiona a exigência de ordem judicial prevista no artigo 19 do Marco Civil da Internet para remoção de conteúdos ilícitos, enquanto o segundo discute a obrigação de fiscalização prévia por provedores (como a Google), com argumentos sobre inviabilidade técnica e riscos de censura privada em casos anteriores à lei.

Na decisão proferida em 26 de junho de 2025, o STF declarou a parcial inconstitucionalidade do artigo 19 do MCI (RE 1037396<sup>152</sup> e RE 1057258<sup>153</sup>), que originalmente condicionava a responsabilização civil de plataformas à prévia ordem judicial. A Corte estabeleceu novo parâmetro: as plataformas passam a poder ser responsabilizadas civilmente se, após notificação extrajudicial, não removerem conteúdos posteriormente considerados ilícitos por decisão judicial.

A decisão também trouxe exceções importantes: em casos de racismo, terrorismo, violência contra mulheres e crianças, ou ataques à democracia, a remoção deve ser imediata, independentemente de ordem judicial, sob pena de responsabilização por falha sistêmica. Já nos crimes contra a honra, mantém-se a exigência de ordem judicial para a responsabilização, embora se permita a remoção voluntária via notificação extrajudicial (Brasil, STF, 2025).

Além disso, a Suprema Corte impôs novos deveres de transparência às plataformas, como a criação de canais de denúncia acessíveis, a publicação de relatórios anuais de moderação de conteúdo e a manutenção de representação legal no Brasil com poderes judiciais. A decisão inovou ao atribuir presunção automática de responsabilidade em casos de conteúdo impulsionado artificialmente por robôs ou algoritmos opacos (Brasil, STF, 2025).

Embora ministros dissidentes tenham defendido a constitucionalidade integral do artigo 19 por receio de estimular censura privada, a maioria da Corte entendeu que a atualização interpretativa era necessária para proteger direitos fundamentais no ambiente digital. Ao final, o STF convocou o Congresso Nacional a elaborar legislação específica, sublinhando que a regulação digital deve ser guiada por um equilíbrio entre inovação tecnológica e proteção constitucional de direitos (Brasil, STF, 2025).

Analisando o contexto da decisão do STF de forma crítica, podemos inferir que ao reinterpretar o artigo 19 do MCI deve ser compreendida não como um episódio isolado de ativismo judicial, mas como sintoma de um descompasso estrutural entre a velocidade das

---

<sup>152</sup> O STF reconheceu a inconstitucionalidade parcial do artigo 19 do Marco Civil da Internet, ao concluir que sua regra geral, exigência de ordem judicial para responsabilização civil de plataformas, é insuficiente para proteger direitos fundamentais e a democracia. A Corte fixou novo entendimento: provedores poderão ser responsabilizados se, após notificação extrajudicial, não removerem conteúdos posteriormente considerados ilícitos. Para crimes graves (como racismo, terrorismo, violência contra mulheres e crianças), a remoção deve ser imediata, sob pena de responsabilização por falha sistêmica. Além disso, estabeleceu-se presunção de responsabilidade em casos de conteúdo impulsionado por bots ou anúncios pagos, e impuseram-se deveres de transparência, canais de denúncia acessíveis e representação legal no Brasil. Os efeitos da decisão são prospectivos e a responsabilidade permanece subjetiva. BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n. 1037396/SP. Relator: Min. Dias Toffoli. Brasília, DF, julgado em 26 jun. 2025. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549>. Acesso em: 11 jul. 2025.

<sup>153</sup> BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n. 1057258/MG. Relator: Min. Luiz Fux. Brasília, DF, julgado em 26 jun. 2025. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5217273>. Acesso em: 11 jul. 2025.

transformações tecnológicas e a morosidade institucional dos procedimentos legislativo brasileiro.

Ao estabelecer novos parâmetros de responsabilidade civil das plataformas, reforçar deveres de transparência algorítmica e disciplinar mecanismos de moderação de conteúdo, a Corte exerceu uma função normativa atípica, própria de contextos excepcionais. Tal atuação, embora juridicamente justificável diante da omissão legislativa, sinaliza a consolidação de um modelo emergente de "jurisdição de exceção" aplicada aos temas digitais.

Esse fenômeno revela a crescente judicialização da política tecnológica e expõe os limites da tradição normativa fragmentada e casuística que prevalece no Brasil, como evidenciado pelas trajetórias da LGPD e do próprio MCI. A atuação do STF, neste contexto, evidencia um deslocamento da centralidade legislativa para o Poder Judiciário, o que compromete o ideal de separação de poderes e, sobretudo, fragiliza a capacidade deliberativa do Parlamento diante do poder assimétrico das *big techs*.

Caso o Congresso permaneça inerte, corre-se o risco de cristalizar um cenário de irrelevância normativa do Legislativo, agravando a reatividade do sistema jurídico e sua suscetibilidade à captura por *lobbies* corporativos transnacionais. A resposta institucional ao vácuo regulatório no ambiente digital exige mais do que ajustes pontuais ou revisões fragmentadas de dispositivos legais. Impõe-se a construção de um novo paradigma normativo, orientado por princípios estruturantes e dotado de vocação integradora e adaptabilidade tecnológica.

A União Europeia tem sido referência, em termos regulatórios, ao adotar um modelo de correção colaborativa, envolvendo Estado, setor privado e sociedade civil. Nesse sentido, uma possível solução seria a criação de um Código Brasileiro de Direito Digital, com o objetivo de unificar temas centrais da regulação digital, como proteção de dados, inteligência artificial, moderação algorítmica e combate à desinformação, em sintonia com modelos internacionais baseados em direitos humanos, como o Marco Digital Europeu.

O Brasil aderiu aos princípios da OCDE para a IA, que reforçam valores como humanocentrismo, equidade, transparência e responsabilidade. Filho e Ladeira (2021, p. 91), lecionam que esses compromissos foram incorporados pela diplomacia brasileira, indicando uma crescente convergência com o padrão regulatório dos países do chamado “núcleo normativo ocidental”.

A superação da atual fragmentação legislativa requer uma arquitetura normativa principiológica, capaz de resistir à obsolescência diante das rápidas transformações tecnológicas e de assegurar a efetividade dos direitos fundamentais no ecossistema digital.



Esse possível Marco regulatório (Novo Código) deveria ser estruturado em Parte Geral, consagrando princípios como dignidade digital, autodeterminação informativa, transparência algorítmica e soberania tecnológica, e em Partes Especiais, voltadas a temas específicos como a regulação da inteligência artificial, a responsabilidade das plataformas digitais, a proteção de dados pessoais e os crimes informacionais.

Tal iniciativa permitiria ao Brasil consolidar um modelo jurídico contemporâneo, democrático e funcional, apto a enfrentar os desafios regulatórios da era algorítmica com coerência, segurança jurídica e foco na proteção dos direitos fundamentais.

## **6.2 Elevação da proteção de dados à direito fundamental**

A proteção de dados pessoais no Brasil chega de forma relativamente tardia, fundamentando-se inicialmente em dispositivos fragmentados no artigo 5º da Constituição Federal de 1988, como o direito à privacidade (inciso X), o sigilo das comunicações e dados (inciso XII) e o *habeas data* para acesso e retificação de registros públicos (inciso LXXII). Esses dispositivos, embora importantes, não formavam um sistema jurídico completo e coeso voltado à proteção informacional na era digital.

Essa lacuna foi acentuada por uma interpretação restritiva do STF, que limitou a aplicação da proteção constitucional apenas aos dados em trânsito, ignorando os riscos relacionados às informações armazenadas ou processadas. Como destaca Doneda (2020, p. 270), embora tradicionalmente vinculada à privacidade, a proteção de dados deve ser compreendida como um direito autônomo, dada a complexidade e ubiquidade do tratamento informatizado na sociedade contemporânea.

Segundo o autor, é necessário reinterpretar de forma integrada as garantias constitucionais já existentes, reconhecendo a proteção de dados como instrumento essencial à tutela da personalidade na era digital (Doneda, 2020, p. 270).<sup>154</sup>

Essa posição é reforçada por Sarlet (2020, p. 187), que argumenta que o direito à proteção de dados pessoais, embora não expresso na CF/88, estava implicitamente positivado no texto constitucional. A Constituição assegura o sigilo de dados e o *habeas data*, mas não protege os dados em si, o que gerou debates sobre sua natureza jurídica. Ainda assim, a doutrina majoritária passou a reconhecer esse direito como fundamental, assentado no princípio da

---

<sup>154</sup> DONEDA, Danilo Cesar Maganhoto. Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados. Revista dos Tribunais. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

dignidade da pessoa humana, no livre desenvolvimento da personalidade e nos direitos à intimidade e privacidade, formando assim uma base constitucional sólida para a sua afirmação como direito autônomo.<sup>155</sup>

Complementando essa análise, o próprio conceito de “dados pessoais” traz implicações relevantes para a compreensão jurídica e técnica do tema. Conforme ressalta Sarlet (2020, p. 52), embora a legislação trate dados e informações como termos equivalentes para fins normativos, há uma distinção conceitual fundamental entre eles: dados são elementos brutos e formalizados, processáveis por sistemas computacionais, enquanto informação surge da interpretação desses dados em um contexto comunicativo.

Essa distinção, embora não afete diretamente a aplicação prática da LGPD, é tecnicamente relevante: nem toda informação é um dado estruturado, e os dados só adquirem sentido quando integrados a um sistema de significado. Assim, mesmo com uma definição jurídica ampla e funcional, a compreensão da natureza técnica dos dados protegidos continua essencial para a construção de políticas e interpretações jurídicas adequadas.

No Brasil, embora a Constituição de 1988 já previsse, de forma indireta, a proteção de dados pessoais por meio de garantias como o *habeas data*, a privacidade e a intimidade, foi apenas em 2020, no julgamento da ADI 6.387, que o STF consolidou o status material de direito fundamental à proteção de dados. Ao declarar inconstitucional a medida provisória que autorizava o compartilhamento desproporcional de dados pessoais, o STF não apenas reafirmou os limites constitucionais ao poder estatal, como também reconheceu esse direito como cláusula de eficácia limitada, aplicável imediatamente e sujeita a limites materiais de reforma constitucional (Acioly; Silva; Neto, 2024, p. 8).<sup>156</sup>

Esse reconhecimento jurisprudencial abriu caminho para a formalização expressa do direito à proteção de dados na ordem constitucional brasileira. Essa formalização ocorreu com a promulgação da Emenda nº 115/2022<sup>157</sup>, que introduziu o inciso LXXIX ao artigo 5º da

<sup>155</sup> SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988. Direitos Fundamentais & Justiça, 2020.

<sup>156</sup> ACIOLY, Luís Enrique de Menezes; SILVA, Matheus Fernandes da; NETO, João Araújo Monteiro. A Emenda Constitucional nº 115 de 10 de fevereiro de 2022 e a aplicação da proteção de dados pessoais no Brasil. Revista de Investigações Constitucionais, v. 3, pág. 7, 2024.

<sup>157</sup> Apesar do avanço normativo constitucional, Furtado (2022, p. 19), em consonância com Sarlet (2020, p. 187), apresenta reflexão interessante ao expor crítica à EC 115/2022 por considerar que a proteção de dados pessoais já está garantida constitucionalmente (via privacidade e dignidade) e que a emenda, além de desnecessária, é prejudicial por promover a inflação de direitos, fragilizar a Constituição e incentivar uma visão exegética ultrapassada. A solução adequada, segundo o autor, está na aplicação de uma hermenêutica jurídica criativa e adaptativa sobre os direitos fundamentais existentes, sempre pautada pela racionalidade jurídica para evitar mudanças constitucionais injustificadas. FURTADO, Samuel Nunes et al. Críticas à EC 115/2022: a proteção de dados pessoais como direito fundamental intrínseco à privacidade. 2022.

Constituição, reconhecendo a proteção de dados pessoais, inclusive nos meios digitais, como direito fundamental autônomo. A emenda também alterou o artigo 22, incluindo o inciso XXX, que atribuiu competência privativa à União para legislar sobre a matéria, afastando a possibilidade de regulação concorrente por Estados e Municípios.

A centralização legislativa e fiscalizatória prevista na EC nº 115/2022 teve como consequência direta o fortalecimento da ANPD como órgão responsável pela governança regulatória do setor. Estruturada como autarquia especial com autonomia técnica e decisória, a ANPD atua com base nos princípios da transparência, responsabilização e da abordagem baseada em risco. Suas atribuições se distribuem em três eixos: preventivo (com emissão de diretrizes e realização de estudos), fiscalizatório (com aplicação de sanções) e regulatório (com edição de normas técnicas e guias interpretativos), incentivando inclusive a autorregulação setorial proporcional à gravidade dos riscos (Acioly; Silva; Neto, 2024, p. 16).

Como reforçam os mesmos autores, a EC nº 115 constitucionalizou o sistema de proteção de dados, conferindo hierarquia máxima e estabilidade à política pública nessa área sensível:

(...) a Emenda Constitucional n. 115, de 2022, teve o condão de elevar ao status de questão constitucional não somente o direito materialmente fundamental, mas o próprio sistema normativo e fiscalizatório, representado em um órgão administrativo central, de competência privativa da União, como já delineado na LGPD, evitando-se a fragmentação do enforcement da proteção de dados pessoais (Acioly; Silva; Neto, 2024, p. 10).<sup>158</sup>

O sistema regulatório atual surge de um processo dinâmico: adaptação de normas existentes, criação de leis novas e, sobretudo, reinterpretção da Constituição de 1988 pelo STF frente a desafios emergentes.

O marco normativo da EC resulta de um processo contínuo de transformação constitucional, iniciado com a releitura da Constituição de 1988 pelo STF frente aos desafios da sociedade informacional. Os fundamentos para a regulação digital derivam do próprio artigo 5º, que, além de proteger a intimidade<sup>159</sup> (inciso X) e garantir o *habeas data* (inciso LXXII), articula-se com o direito de propriedade (inciso XXII), cuja função social (inciso XXIII) passa

<sup>158</sup> ACIOLY, Luís Enrique de Menezes; SILVA, Matheus Fernandes da; NETO, João Araújo Monteiro. A Emenda Constitucional nº 115 de 10 de fevereiro de 2022 e a aplicação da proteção de dados pessoais no Brasil. *Revista de Investigações Constitucionais*, v. 3, pág. 7, 2024.

<sup>159</sup> Conforme Martins (2024), a intimidade e vida privada são expressões do direito de estar só, protegendo a esfera reservada do indivíduo. A vida privada é mais ampla, abrangendo todas as relações sociais (como trabalho e estudo), enquanto a intimidade refere-se estritamente às relações pessoais e afetivas (família e amigos próximos). MARTINS, Flavio. *Curso de Direito Constitucional*. 8. ed. São Paulo: Saraiva, 2024.

a informar também a regulação de ativos digitais e dados pessoais como bens jurídicos relevantes.

Nesse sentido, a EC nº 115<sup>160</sup> representa não apenas uma atualização formal do texto constitucional, mas a consagração de um novo paradigma: o de que a proteção de dados é central para a tutela da dignidade humana na era digital, exigindo do Estado ações coordenadas, competência normativa exclusiva e uma autoridade reguladora eficaz.

De acordo com estudo conduzido por Abreu (2024, p. 12) anteriormente, constata-se que a jurisprudência do STF sobre sigilo de dados evoluiu de uma proteção ampla (Ação Penal 30 de 1994, caso Collor<sup>161</sup>) para uma distinção crucial entre "comunicação de dados" e "dados armazenados". Enquanto no caso Collor predominou a tese de inviolabilidade absoluta de dados em computadores, o RE 418.416<sup>162</sup> estabeleceu que o artigo 5º, XII da CF protege apenas fluxos comunicativos, não dados estáticos. Essa virada foi consolidada no HC 91.867<sup>163</sup>, que permitiu o acesso a registros telefônicos em aparelhos apreendidos, fundamentando que metadados armazenados não gozam da proteção constitucional do sigilo de comunicações.<sup>164</sup>

Esse recorte restritivo impulsionou o desenvolvimento doutrinário em defesa de uma proteção de dados mais ampla e autônoma. Segundo Sarlet (2020, p. 47), embora vinculado à dignidade da pessoa humana, à privacidade e à autodeterminação informativa, o direito fundamental à proteção de dados possui densidade própria. Sua essência reside na proteção preventiva e integral de dados pessoais enquanto projeções da personalidade, reconhecendo que sua manipulação inadequada pode violar direitos mesmo sem divulgação.

Nesse sentido, a proteção de dados não se confunde com a privacidade tradicional, centrada na exclusão do outro ("estar só"), nem se reduz à autodeterminação informativa, que garante o controle individual, mas admite restrições pelo interesse coletivo. Trata-se de um direito autônomo, com dimensão coletiva estruturante da esfera pública digital e da própria ordem democrática (Sarlet, 2020, p. 50).<sup>165</sup>

<sup>160</sup> 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.

<sup>161</sup> BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Ação Penal n. 307/DF. Relator: Min. Ilmar Galvão, 13 de dezembro de 1994. Diário de Justiça, 13 de outubro de 1995.

<sup>162</sup> BRASIL. Supremo Tribunal Federal (Tribunal Pleno). Recurso Extraordinário n. 418.416/SC. Relator: Min. Sepúlveda Pertence, 10 de maio de 2006. Diário de Justiça eletrônico, 02 de fevereiro de 2007.

<sup>163</sup> BRASIL. Supremo Tribunal Federal (2. Turma). Habeas Corpus n. 91.867/PA. Relator: Min. Gilmar Mendes, 24 de abril de 2012. Diário de Justiça Eletrônico, 20 de setembro de 2012.

<sup>164</sup> ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. Revista de Investigações Constitucionais, v. 11, n. 1, p. e256, 2024.

<sup>165</sup> SARLET, Ingo Wolfgang; SAAVEDRA, Giovanni Agostini. Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais. Direito Público, [S.l.], v. 17, n. 93, p. 34-57, 2020.

Essa concepção mais robusta foi gradualmente incorporada pelo STF, como se observa no julgamento da ADI 6.649/DF, já anterior à EC nº 115, no qual a Corte afirmou o direito à proteção de dados e à autodeterminação informacional como direitos fundamentais, exigindo que o compartilhamento de dados entre entes públicos respeite finalidades legítimas, limitação ao necessário e compatibilidade com os propósitos declarados<sup>166</sup>:

O STF reconheceu o direito fundamental à proteção de dados e à autodeterminação informacional, posteriormente positivado no Art. 5º, LXXIX, pela EC 115/2022. A Corte rejeitou uma visão dicotômica entre interesse público e privacidade, exigindo que o compartilhamento de dados entre órgãos públicos observe: finalidades legítimas, compatibilidade com os propósitos declarados e limitação ao mínimo necessário. (BRASIL, STF, ADI 6.649/DF e ADPF 695/DF, Rel. Min. Gilmar Mendes, Plenário, j. 01 set. 2022.)

A Suprema Corte aprofundou essa linha em decisões como a ADI 4.906, validando o compartilhamento de dados cadastrais genéricos para fins de investigação criminal, sem autorização judicial prévia, por entender que tais dados não integram o núcleo protegido pelo sigilo de comunicações:

O objeto de tutela mediante a imposição de sigilo não alcança os dados cadastrais. O direito fundamental à proteção de dados e à autodeterminação informativa (...) impõe a adoção de mecanismos capazes de assegurar a proteção e a segurança dos dados pessoais manipulados pelo poder público e por terceiros. É compatível com a Constituição de 1988 o compartilhamento direto de dados cadastrais genéricos com os órgãos de persecução penal, para fins de investigação criminal, mesmo sem autorização da Justiça. (Brasil, STF, ADI 4906, Rel. Min. Nunes Marques, Tribunal Pleno, j. 11 set. 2024, DJe 24 out. 2024.<sup>167</sup>

Contudo, em decisões como o HC 222.141 AgR, o Tribunal estabeleceu limites rigorosos para acessar conteúdos sensíveis ou registros de conexão, exigindo, como regra, ordem judicial específica<sup>168</sup>:

---

Disponível em: <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315>. Acesso em: 22 jun. 2025.

<sup>166</sup> BRASIL. Supremo Tribunal Federal (Plenário). Ação Direta de Inconstitucionalidade 6.649/DF. Relator: Min. Gilmar Mendes, 15 set. 2022. Diário de Justiça Eletrônico, Brasília, DF, 19 jun. 2023. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>. Acesso em: 22 abr. 2025. Acesso em: 22 abr. 2025.

<sup>167</sup> BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 4906. Relator: Ministro Nunes Marques, julgado em 11 set. 2024. Diário da Justiça Eletrônico, s/n, divulgado em 23 out. 2024, publicado em 24 out. 2024. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur515682/false>. Acesso em: 24 maio 2025.

<sup>168</sup> BRASIL. Supremo Tribunal Federal. Segunda Turma. Agravo Regimental no Habeas Corpus n. 222.141 Paraná. Relator: Min. Ricardo Lewandowski. Redator para o acórdão: Min. Gilmar Mendes. Julgado em 6 fev. 2024. Publicado em 6 fev. 2024. Disponível em: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/HC222141.pdf>. Acesso em 20 maio 2025.

A disponibilização de dados pessoais, comunicações privadas ou registros de conexão está condicionada à determinação do juiz. A subtração do controle do cidadão sobre suas informações sem autorização judicial configura violação à privacidade. (BRASIL. Supremo Tribunal Federal. HC 222.141 AgR/PR, Rel. Min. Ricardo Lewandowski, Segunda Turma, Julgamento: 06 de fev. de 2024, Publicação: 15 abr. 2024)

Neste último caso, o STF considerou ilícita a requisição de dados sensíveis (e-mails, histórico de busca, geolocalização) feita pelo Ministério Público sem autorização judicial, ainda que o acesso posterior tenha sido autorizado. A Corte reafirmou que a privação do controle do titular sobre seus dados fora das hipóteses legais configura violação direta à autodeterminação informativa, reforçando a necessidade de proporcionalidade e respeito ao devido processo legal, à luz do artigo 5º, LXXIX.<sup>169</sup>

Então, observa-se que a constitucionalização expressa do direito à proteção de dados pela EC nº 115 não apenas reafirma um entendimento já presente na jurisprudência, mas também consolida a LGPD como parâmetro de controle de constitucionalidade. Ao mesmo tempo, impõe limites claros à atuação estatal e privada, exigindo ponderação com outros direitos básicos e fundamentação transparente para qualquer tratamento de dados pessoais.

Para além desse reforço normativo, a EC nº 115 também desempenha um papel simbólico crucial ao consolidar a autodeterminação informativa como dimensão essencial da dignidade humana na era algorítmica. Esse avanço reflete uma "Constituição aberta" e responsiva, característica das democracias contemporâneas, e conecta-se ao objetivo do presente estudo de investigar os "novos direitos" emergentes de transformações tecnológicas globais e da intensificação da participação cidadã em ambientes digitais.

Nesse encadeamento, a proteção de dados transcende o campo das liberdades negativas, exigindo mecanismos inovadores de efetivação positiva, capazes de responder à hipercomplexidade do ecossistema digital. A análise proposta aqui considera três eixos fundamentais de concretização: (i) regulação setorial (LGPD e MCI); (ii) institucionalidade (especialmente o papel da ANPD); e (iii) interpretação jurisprudencial (com destaque para o

---

<sup>169</sup> A Emenda Constitucional n.º 115/2022 promoveu a inclusão do inciso LXXIX no artigo 5º da Constituição Federal. Este dispositivo legal estabelece, de forma explícita, o direito à proteção de dados pessoais, abrangendo os meios digitais. A relevância jurídica do acesso a dados pessoais, especialmente no ambiente digital, não era totalmente apreendida no momento da promulgação do texto constitucional original: art. 5º, CF/88: “LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)”. Contudo, a evolução tecnológica, caracterizada pela informatização e pela disseminação instantânea de informações eletrônicas, introduziu novas questões relativas à intimidade, segurança e privacidade do cidadão no que tange ao tratamento, armazenamento, transmissão e sigilo dos dados. BRASIL. Constituição da República Federativa do Brasil de 1988. Art. 5º, inciso LXXIX. Incluído pela Emenda Constitucional nº 115, de 10 de fevereiro de 2022.

STF), os quais demonstram como o direito à proteção de dados se articula com uma infraestrutura normativa e institucional proativa.

A EC nº 115 também materializa a busca por igualdade substantiva no ciberespaço, ao coibir assimetrias de poder informacional entre titulares de dados e grandes conglomerados digitais. Essa mudança estrutural permite problematizar tensões entre inovação tecnológica e garantias fundamentais, evidenciando lacunas na proteção de grupos vulneráveis, como crianças em plataformas digitais, e impulsionando propostas de modelos de governança que equilibrem eficiência sistêmica e emancipação individual.

Nesse cenário, a constitucionalização da proteção de dados fortalece a aplicação concreta da LGPD, legitima a atuação normativa e fiscalizatória da ANPD e impõe deveres positivos aos entes públicos e privados. Esses agentes, agora, não apenas devem evitar violações, mas também demonstrar responsabilidade ativa e diligência na gestão de dados pessoais. Isso implica uma transição necessária de um modelo jurídico reativo para um modelo estrutural e antecipatório, articulando o direito fundamental à proteção de dados com políticas públicas robustas, fiscalização eficaz e participação cidadã informada.

Por fim, compreende-se que a proteção de dados na era digital ultrapassa o plano normativo-legal, tornando-se um imperativo democrático essencial. Ela atua como barreira contra o autoritarismo algorítmico, mecanismo de contenção do abuso de poder informacional, e instrumento de promoção da pluralidade informativa e da igualdade de oportunidades no ambiente digital.

Sua efetividade, no entanto, dependerá da mobilização coordenada entre instituições públicas, sistema de justiça e sociedade civil, rumo a um ciberespaço mais ético, equitativo e compatível com os valores constitucionais da dignidade humana.

## 7 CONSIDERAÇÕES FINAIS

A presente investigação acadêmica procedeu à análise da evolução normativa do Direito Digital brasileiro, abrangendo o período desde a formação da indústria de informática até a constitucionalização da proteção de dados.

Observou-se a segmentação deste processo dinâmico e dialético em três fases principais – *hardware*, *software* e dados – as quais se correlacionam com os modos pelos quais o Estado brasileiro buscou adaptar-se aos impactos sucessivos da informatização, digitalização e da economia algorítmica.

A metodologia empregada foi de natureza qualitativa, utilizando a triangulação entre fontes normativas, jurisprudência e doutrina. Esta abordagem possibilitou a construção de uma linha crítica da regulação digital no país, com foco na historicidade e funcionalidade normativa.

A análise revelou que o processo regulatório não se manifestou de maneira linear ou coesa, sendo marcado por movimentos predominantemente reativos, respostas fragmentadas, ausência de integração institucional e tensões inerentes à soberania estatal frente à transnacionalidade das infraestruturas digitais.

A primeira fase, compreendida entre 1950 e 1990, foi caracterizada por políticas protecionistas centradas na criação de órgãos como a CAPRE e a SEI. Este período culminou na Lei da Reserva de Mercado de informática. Embora motivada pela busca de soberania tecnológica, tal política resultou em um ecossistema regulatório fragmentado, marcado pela centralização estatal e limitada integração entre *hardware*, *software* e inovação.

A segunda fase, abrangendo o período de 1990 a 2010, é correlata à denominada "Revolução do *Software*". Esta fase foi inaugurada pela Lei nº 9.609/1998, que normatizou os programas de computador, além de registrar avanços pontuais em propriedade intelectual e comércio eletrônico. Contudo, manteve-se a lógica de respostas normativas setoriais e pontuais, sem a antecipação dos desafios transversais que seriam impostos pela emergente economia de dados.

A terceira fase, em curso desde 2010, representa um salto qualitativo com a instituição de marcos sistêmicos como o Marco Civil da Internet em 2014 e a Lei Geral de Proteção de Dados em 2018. Esta fase foi consolidada pela Emenda Constitucional nº 115 em 2022, que elevou a proteção de dados ao *status* de direito fundamental. Essa transformação reflete uma inflexão normativa, que reposiciona o Estado como garantidor de direitos na era digital.

Apesar dos avanços observados na regulação do Direito Digital brasileiro, persistem três dilemas regulatórios centrais: a desarticulação entre normas setoriais, a ausência de uma



governança coordenada em temas emergentes como a IA e as plataformas digitais, e a dificuldade em alinhar os princípios constitucionais à lógica transnacional e opaca dos algoritmos.

A fragmentação legislativa no tocante à IA, evidenciada por diversos projetos de lei sobrepostos e desconectados do sistema constitucional de direitos, expressa a permanência de um modelo regulatório compartimentalizado, que guarda herança da política industrial estabelecida na década de 1980.

A pesquisa evidenciou que a eficácia do marco regulatório não se restringe à produção legislativa, dependendo intrinsecamente da capacidade responsiva de instituições como a Autoridade Nacional de Proteção de Dados, da robustez da segurança cibernética pública e da definição de critérios claros para coibir abusos praticados pelas grandes plataformas digitais.

Neste cenário, a atuação do Supremo adquire relevância na reinterpretação dos princípios constitucionais sob a ótica da realidade digital. Contudo, a falta de uniformidade interpretativa e a escassez de precedentes vinculantes limitam a construção de um regime jurídico sólido, estável e eficaz.

A análise revelou, ademais, um descompasso estrutural entre a velocidade da inovação tecnológica e a morosidade do processo normativo. O trâmite do Projeto de Lei nº 2.630/2022 ilustra este impasse, ao mesmo tempo em que expõe as tensões entre regulação estatal, liberdade de expressão e o poder concentrado das *big techs*.

Em face deste contexto, soluções como a correção regulatória orientada por direitos humanos e a aplicação de princípios flexíveis despontam como caminhos viáveis. Não obstante, permanecem desafios significativos: a persistência da fragmentação normativa, a questão da extraterritorialidade das plataformas e os riscos inerentes a um regime autorregulado, pautado predominantemente por interesses privados.

Conclui-se que a trajetória do Direito Digital no Brasil, embora marcada por conquistas relevantes, a exemplo da constitucionalização da proteção de dados e da criação da ANPD, ainda carece de coerência sistêmica, densidade normativa e capacidade regulatória proativa.

A superação deste quadro exige a instituição de um novo paradigma jurídico e institucional, fundamentado em governança multissetorial, racionalidade prospectiva e densificação dos princípios constitucionais, notadamente a dignidade da pessoa humana, a autodeterminação informativa, a liberdade de expressão e a proteção contra abusos algorítmicos.

A investigação finaliza com a constatação de que o ordenamento jurídico brasileiro ainda se encontra em fase de construção no que concerne à regulação digital. Registrou-se, com

efeito, avanço na proteção de dados e na estruturação institucional, mas a predominância de um modelo reativo, setorial e fragmentado compromete a edificação de um regime jurídico capaz de lidar com os desafios complexos e interdependentes da era algorítmica.

O Direito Digital brasileiro não deve ser concebido como um ramo estanque, mas como um campo transversal e estratégico, no qual se define o modelo de sociedade a ser edificado na era informacional. O êxito deste projeto nacional não dependerá da importação de soluções exógenas, mas da edificação de um marco regulatório próprio, ancorado nos nossos valores constitucionais.

## 8 REFERÊNCIAS

- ABREU, Jacqueline de Souza. Comunicação de dados, não dados em si: origens e problemas do atual paradigma de proteção constitucional do sigilo de dados. *Revista de Investigações Constitucionais*, v. 11, n. 1, p. e256, 2024.
- ACIOLY, Luís Enrique de Menezes; SILVA, Matheus Fernandes da; NETO, João Araújo Monteiro. A Emenda Constitucional nº 115 de 10 de fevereiro de 2022 e a aplicação da proteção de dados pessoais no Brasil. *Revista de Investigações Constitucionais*, v. 3, pág. 7, 2024.
- ADAMOPOULOU, Eleni; MOUSSIADES, Lefteris. Chatbots: História, tecnologia e aplicações. *Aprendizado de Máquina com Aplicações*, v. 2, p. 100006, 2020.
- ASIANOMETRY. Brazil Tried to Protect Its Computer Industry. 2023. [Vídeo] – Vídeo (23min25s). Disponível em: <https://www.youtube.com/watch?v=brOtbWIViWM>. Acesso em: 23 maio 2025.
- BARBOSA, Denis Borges. *A Proteção do Software*. DBBA, 2018.
- BARBOSA, Leonardo Figueiredo; PINHEIRO, Caroline da Rosa. Inteligência artificial no Brasil: avanços regulatórios. *Revista de Informação Legislativa*, v. 60, n. 240, p. 11-41, 2023. [https://doi.org/10.70015/ril\\_v60\\_n240\\_p11](https://doi.org/10.70015/ril_v60_n240_p11)
- BEIGUELMAN, Giselle. As verdades dos deepfakes. *Revista Zum*, v. 18, pág. 50-58, 2020.
- BELLI, Luca et al. *Cibersegurança*. 2023.
- BIONI, Bruno; GARROTE, Marina; GUEDES, Paula. *Temas centrais na Regulação de IA: O local, o regional e o global na busca da interoperabilidade regulatória*. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2023.
- BRASIL. Agência Nacional de Vigilância Sanitária (Anvisa). Anvisa adota estratégia baseada em inteligência artificial para otimizar análise de medicamentos. 2024. Disponível em: <https://www.gov.br/anvisa/pt-br/assuntos/noticias-anvisa/2024/anvisa-adota-estrategia-baseada-em-inteligencia-artificial-para-otimizar-analise-de-medicamentos>. Acesso em: 23 maio 2025.
- BRASIL. Associação Brasileira da Indústria Elétrica e Eletrônica (ABINEE). Website Institucional. São Paulo: ABINEE, 2023. Disponível em: <https://www.abinee.org.br/>. Acesso em: 12 maio 2025.
- BRASIL. Associação Brasileira De Normas Técnicas (ABNT). ABNT NBR ISO/IEC 27001: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2022a.
- BRASIL. Associação Brasileira De Normas Técnicas (ABNT). ABNT NBR ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação. Rio de Janeiro: ABNT, 2022b.

BRASIL. Câmara Dos Deputados. Marco Civil da Internet: análise da Lei nº 12.965/2014. Brasília, DF, 2014. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/estudos-e-notas-tecnicas/publicacoes-da-consultoria-legislativa/estudos-e-notas-tecnicas-1/direito-constitucional-e-justica/marco-civil-da-internet-analise-da-lei-no-12-965-2014>. Acesso em: 12 maio 2025.

BRASIL. Conselho Monetário Nacional. Resolução nº 4.658, de 26 de abril de 2018. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Diário Oficial da União, Brasília, DF, 27 de abr. 2018.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 12 maio 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. Art. 5º, inciso LXXIX. Incluído pela Emenda Constitucional nº 115, de 10 de fevereiro de 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 20 maio 2025.

BRASIL. Decreto nº 47.701, de 26 de agosto de 1960. Dispõe sobre a organização dos serviços de processamento de dados na administração federal. Diário Oficial da União, Brasília, DF, 27 ago. 1960. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1960-1969/decreto-47701-22-janeiro-1960-387087-publicacaooriginal-1-pe.html>. Acesso: 23 maio 2025.

BRASIL. Decreto nº 70.370, de 5 de abril de 1972. Câmara dos Deputados - legislação. Disponível em: <https://www2.camara.leg.br/legin/fed/decret/1970-1979/decreto-70370-5-abril-1972-418827-publicacaooriginal-1-pe.html>. Acesso: 13 abr. de 2025.

BRASIL. Decreto nº 7.962, de 15 de março de 2013. Regulamenta a Lei nº 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2013/decreto/d7962.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm). Acesso em: 18 maio 2025.

BRASIL. Decreto nº 84.067, de 2 de outubro de 1979. Cria a Secretaria Especial de Informática e dá outras providências. Diário Oficial da União, Brasília, DF, 3 out. 1979. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/decreto/1970-1979/d84067.htm#:~:text=DECRETO%20No%2084.067%2C%20DE,Nacional%2C%20e%20d%C3%A1%20outras%20provid%C3%AAs](https://www.planalto.gov.br/ccivil_03/decreto/1970-1979/d84067.htm#:~:text=DECRETO%20No%2084.067%2C%20DE,Nacional%2C%20e%20d%C3%A1%20outras%20provid%C3%AAs). Acesso em: 02 de abr. de 2025.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso

IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/decreto/d9637.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm). Acesso em: 24 maio 2025.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/decreto/d10222.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm). Acesso em: 12 maio 2025.

BRASIL. Decreto nº 10.278, de 18 de março de 2020. Regulamenta a Lei nº 13.874, de 20 de setembro de 2019, e a Lei nº 12.682, de 9 de julho de 2012. Diário Oficial da União, Brasília, DF, 19 mar. 2020. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/decreto/D10278.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10278.htm). Acesso em: 12 maio 2025.

BRASIL. Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/decreto/d10332.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10332.htm). Acesso em: 24 maio 2025.

BRASIL. Decreto nº 10.356, de 20 de maio de 2020. Regulamenta a Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a Política Nacional de Informática. Diário Oficial da União, Brasília, DF, 21 maio 2020. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2020/Decreto/D10356.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/Decreto/D10356.htm). Acesso em: 12 maio 2025.

BRASIL. Decreto nº 5.906, de 26 de setembro de 2006. Regulamenta a Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a Política Nacional de Informática. Diário Oficial da União, Brasília, DF, 27 set. 2006. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2004-2006/2006/decreto/d5906.htm](http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/decreto/d5906.htm). Acesso em: 12 maio 2025.

BRASIL. Decreto-lei nº 200, de 25 de fevereiro de 1967. Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Diário Oficial da União, Brasília, DF, 27 fev. 1967. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/decreto-lei/del0200.htm](https://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm). Acesso: 23 maio 2025.

BRASIL. Decreto-Lei nº 1.209, de 2 de outubro de 1972. Concede incentivos fiscais para programas especiais de desenvolvimento e dá outras providências. Diário Oficial da União, Brasília, DF, 3 out. 1972. Disponível em: <https://www2.camara.leg.br/legin/fed/declei/1970-1979/decreto-lei-1209-28-fevereiro-1972-375353-publicacaooriginal-1-pe.html>. Acesso: 23 maio 2025.

BRASIL. Decreto-Lei nº 1.219, de 15 de maio de 1972. Dispõe sobre a concessão de estímulos à exportação de manufaturados e dá outras providências. Disponível em: <https://www2.camara.leg.br/legin/fed/declei/1970-1979/decreto-lei-1209-28-fevereiro-1972-375353-publicacaooriginal-1-pe.html>. Acesso em: 23 maio 2025.

BRASIL. Emenda Constitucional nº 85, de 26 de fevereiro de 2015. Altera e adiciona dispositivos na Constituição Federal para atualizar o tratamento das atividades de ciência,

tecnologia e inovação. Disponível

em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/Emendas/Emc/emc85.htm#art1](https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc85.htm#art1).

Acesso em: 20 maio 2025.

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. Disponível em:

[https://www.planalto.gov.br/ccivil\\_03/constituicao/Emendas/Emc/emc115.htm#art1](https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#art1). Acesso em: 23 maio 2025.

BRASIL. Instituto Nacional da Propriedade Industrial (INPI). Guia Básico de

Patente. Disponível em: <https://www.gov.br/inpi/pt-br/servicos/patentes/guia-basico>. Acesso em: 12 maio 2025.

BRASIL. Instituto Nacional da Propriedade Industrial (INPI). Manual de Marcas. Disponível em: <https://manualdemarcas.inpi.gov.br/>. Acesso em: 24 maio 2025.

BRASIL. Instituto Nacional Da Propriedade Industrial (INPI). Manual de Desenho Industrial. Rio de Janeiro: INPI, 2021. Disponível em: <https://manualdemarcas.inpi.gov.br/>. Acesso em: 12 maio 2025.

BRASIL. Inovação UNB. O que pode ser protegido pelo desenho industrial. Disponível em: <https://inovacao.unb.br/o-que-pode-ser-protetido-pelo-registro-de-desenho-industrial/>.

Acesso em: 23 maio 2025.

BRASIL. Lei nº 5.988, de 14 de dezembro de 1973. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da União, Brasília, DF, 17 dez. 1973. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l5988.htm](http://www.planalto.gov.br/ccivil_03/leis/l5988.htm). Acesso em: 12 maio 2025.

BRASIL. Lei nº 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Planalto Legislação, 1984. Disponível em: [https://www.planalto.gov.br/CCivil\\_03/leis/L7232.htm](https://www.planalto.gov.br/CCivil_03/leis/L7232.htm). Acesso em: 23 maio 2025

BRASIL. Lei nº 7.646, de 18 de dezembro de 1987. Dispõe sobre a proteção de propriedade intelectual de programa de computador e sua comercialização no País. Diário Oficial da União, Brasília, DF, 21 dez. 1987. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l7646.htm](http://www.planalto.gov.br/ccivil_03/leis/l7646.htm). Acesso em: 12 maio 2025.

BRASIL. Lei nº 8.248, de 23 de outubro de 1991. Dispõe sobre a Política Nacional de Informática. Diário Oficial da União, Brasília, DF, 24 out. 1991. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/l8248.htm](http://www.planalto.gov.br/ccivil_03/leis/l8248.htm). Acesso em: 12 maio 2025.

BRASIL. Lei nº 8.387, de 30 de dezembro de 1991. Dá nova redação ao § 1º do art. 3º aos arts. 7º e 9º do Decreto-Lei nº 288, de 28 de fevereiro de 1967, ao caput do art. 37 do Decreto-Lei nº 1.455, de 7 de abril de 1976 e ao art. 10 da Lei nº 2.145, de 29 de dezembro de 1953, e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/L8387.htm](https://www.planalto.gov.br/ccivil_03/leis/L8387.htm). Acesso em: 24 maio 2025.

BRASIL. Lei nº 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Brasília, DF, 14 maio de 1996. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/19279.htm](https://www.planalto.gov.br/ccivil_03/leis/19279.htm). Acesso em: 01 mar. 2025.

BRASIL. Lei nº 9.507, de 12 de novembro de 1997. Dispõe sobre o direito de acesso a informações e disciplina o rito processual do habeas data. Diário Oficial da União, Brasília, DF, 13 nov. 1997. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/19507.htm](https://www.planalto.gov.br/ccivil_03/leis/19507.htm). Acesso em: 12 maio 2025.

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, 20 fev. 1998. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/19609.htm](http://www.planalto.gov.br/ccivil_03/leis/19609.htm). Acesso em: 12 maio 2025.

BRASIL. Lei nº 9.610, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/19610.htm](https://www.planalto.gov.br/ccivil_03/leis/19610.htm). Acesso em: 24 maio 2025.

BRASIL. Lei nº 10.176, de 11 de janeiro de 2001. Altera dispositivos da Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a Política Nacional de Informática. Diário Oficial da União, Brasília, DF, 12 jan. 2001. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/leis\\_2001/110176.htm](http://www.planalto.gov.br/ccivil_03/leis/leis_2001/110176.htm). Acesso em: 12 maio 2025.

BRASIL. Lei nº 10.973, de 2 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. 1 Diário Oficial da União, Brasília, DF, 3 dez. 2004. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2004-2006/2004/lei/110.973.htm](http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/110.973.htm). Acesso em: 12 maio 2025.

BRASIL. Lei nº 11.196, de 21 de novembro de 2005. Institui o Regime Especial de Tributação para a Plataforma de Exportação de Serviços de Tecnologia da Informação – REPES, o Regime Especial de Aquisição de Bens de Capital para Empresas Exportadoras – RECAP e o Programa de Inclusão Digital; dispõe sobre incentivos fiscais para a inovação tecnológica. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2004-2006/2005/lei/111196.htm](https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/lei/111196.htm). Acesso em: 24 maio 2025.

BRASIL. Lei nº 11.484, de 31 de maio de 2007. Altera e acresce dispositivos à Lei nº 8.248, de 23 de outubro de 1991, que dispõe sobre a Política Nacional de Informática. Diário Oficial da União, Brasília, DF, 1 jun. 2007. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_Ato2007-2010/2007/Lei/L11484.htm](http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2007/Lei/L11484.htm). Acesso em: 12 maio 2025.

BRASIL. Lei nº 12.529, de 30 de novembro de 2011. Estrutura o Sistema Brasileiro de Defesa da Concorrência; dispõe sobre a prevenção e repressão às infrações contra a ordem econômica; altera a Lei nº 8.137, de 27 de dezembro de 1990, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, e a Lei nº 7.347, de 24 de julho de 1985; revoga dispositivos da Lei nº 8.884, de 11 de junho de 1994, e a Lei nº 9.781, de 19 de janeiro de 1999; e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2011/lei/112529.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/112529.htm). Acesso em: 6 abr. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm). Acesso em: 12 maio 2025.

BRASIL. Lei nº 13.756, de 12 de dezembro de 2018. Dispõe sobre a distribuição da arrecadação das loterias de prognósticos e concursos de números e sobre a autorização para a exploração da modalidade de aposta de quota fixa. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13756compilado.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13756compilado.htm). Acesso em: 01 de abr. de 2025.

BRASIL. Lei nº 13.969, de 26 de dezembro de 2019. Altera a Lei nº 8.248, de 23 de outubro de 1991, para dispor sobre a nova forma de concessão dos incentivos fiscais de que trata a referida Lei. Diário Oficial da União, Brasília, DF, 27 dez. 2019. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2019/lei/L13969.htm](http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13969.htm). Acesso em: 12 maio 2025.

BRASIL. Lei nº 14.063, de 23 de setembro de 2020. Dispõe sobre o uso de assinaturas eletrônicas em comunicações com entes públicos e em negócios jurídicos e dá outras providências. Diário Oficial da União, Brasília, DF, 24 set. 2020. Instituto Nacional de Tecnologia da Informação (ITI). ICP-Brasil. Disponível em: <https://www.gov.br/iti/pt-br/assuntos/icp-brasil>. Acesso em: 12 maio 2025.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2021/lei/114129.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114129.htm). Acesso em: 24 maio 2025.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2021/lei/114155.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/114155.htm). Acesso em: 21 maio 2025.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais e dá outras providências. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2019-2022/2022/lei/114478.htm](https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/114478.htm). Acesso em: 24 maio 2025.

BRASIL. Lei nº 14.790, de 28 de dezembro de 2023. Dispõe sobre as apostas de quota fixa. MINISTÉRIO DA FAZENDA. Legislação - Apostas. <https://www.gov.br/fazenda/pt-br/incorporados/noticias/2024/maio/ministerio-da-fazenda-e-loterias-caixa-vao-regular-apostas-de-quota-fixa-no-brasil>. Acesso em: 12 maio 2025.



BRASIL. Lei nº 14.852, de 6 de maio de 2024. Cria o marco legal para a indústria de jogos eletrônicos. Diário Oficial da União, Brasília, DF, 06 maio 2024. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2023-2026/2024/lei/L14852.htm](http://www.planalto.gov.br/ccivil_03/_ato2023-2026/2024/lei/L14852.htm). Acesso em: 12 maio 2025.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. Portaria MCTI nº 4.979, de 2021. Altera o anexo da Portaria MCTI nº 4.617, de 6 de abril de 2021. Disponível em: [https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-portaria\\_mcti\\_4-979\\_2021\\_anexo1.pdf](https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-portaria_mcti_4-979_2021_anexo1.pdf). Acesso em: 24 maio 2025.

BRASIL. Ministério da Fazenda. Ministério do Planejamento e Coordenação Geral. Portaria Interministerial nº 10, de 17 de janeiro de 1975. Estabelece normas para a concessão de incentivos fiscais à produção de componentes eletrônicos. Diário Oficial da União, Brasília, DF, 20 jan. 1975. Disponível em: <https://www2.camara.leg.br/legin/fed/declei/1970-1979/decreto-lei-1209-28-fevereiro-1972-375353-publicacaooriginal-1-pe.html>. Acesso: 23 maio 2025.

BRASIL. Ministério da Fazenda. Secretaria de Reformas Econômicas. Plataformas Digitais: Aspectos Econômicos e Concorrenciais e Recomendações para Aprimoramentos Regulatórios no Brasil. Brasília, DF: Ministério da Fazenda, 2024. Disponível em: [https://www.gov.br/fazenda/pt-br/central-de-conteudo/publicacoes/apresentacoes/2024/outubro/arquivo/plataformas-digitais-concorrencia\\_10102024-pptx-1.pdf](https://www.gov.br/fazenda/pt-br/central-de-conteudo/publicacoes/apresentacoes/2024/outubro/arquivo/plataformas-digitais-concorrencia_10102024-pptx-1.pdf). Acesso em: 24 maio 2025.

BRASIL. Ministério do Desenvolvimento, Indústria, Comércio e Serviços. Instituto Nacional da Propriedade Industrial. Topografias de Circuitos Integrados. Disponível em: <https://www.gov.br/inpi/pt-br/servicos/topografias-de-circuitos-integrados>. Acesso em: 24 maio 2025.

BRASIL. Ministério do Planejamento e Coordenação Econômica. Portaria nº 322, de 4 de agosto de 1967. Cria o Grupo Executivo para o Desenvolvimento da Indústria de Computadores Eletrônicos - GEDICE, e dá outras providências. Diário Oficial da União, Brasília, DF, 7 ago. 1967. Disponível em: . Acesso em: 2 de abr. de 2025.

BRASIL. Primeira Turma Recursal dos Juizados Especiais Cíveis, Criminais e da Fazenda Pública do Estado do Amazonas. Recurso Inominado Cível nº 0639205-64.2021.8.04.0001. Sala das Sessões, em Manaus, 5 de maio de 2023. Francisco Soares de Souza Relator'. Relator: Juiz Celso Antunes da Silveira Filho. Manaus, AM, 15 de março de 2023. Disponível em: <https://consultasaj.tjam.jus.br/cposgcr/show.do?processo.codigo=P1000457S0000>. Acesso em: 01 abr. 2025.

BRASIL. Portaria nº 5.150, de 2 de outubro de 2018. Dispõe sobre as instruções para elaboração do relatório conclusivo pelas auditorias independentes, na análise dos demonstrativos de cumprimento das obrigações de que trata o § 9º do art. 11 da Lei nº 8.248, de 23 de outubro de 1991 — Manual de Análise do Relatório Demonstrativo Anual (RDA). Disponível em: [https://www.in.gov.br/materia/-/asset\\_publisher/Kujrw0TZC2Mb/content/id/43883676/do1-2018-10-04-portarian-5-150-de-2-de-outubro-de-2018-43883528](https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/43883676/do1-2018-10-04-portarian-5-150-de-2-de-outubro-de-2018-43883528). Acesso em: 16 maio 2025.

BRASIL. Senado Federal. Projeto de Lei nº 21/2020. Dispõe sobre o uso da Inteligência Artificial. Brasília, 2020. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347593&disposition=inline>. Acesso em: 23 maio 2025.

BRASIL. Senado Federal. Projeto de Lei nº 2338/2023. Dispõe sobre o uso da Inteligência Artificial. Brasília, 2023. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1733877727346&disposition=inline#:~:text=1%C2%BA%20Esta%20Lei%20estabelece%20normas,benef%C3%ADcio%20da%20pessoa%20humana%2C%20do>. Acesso em: 05 de abr. de 2025.

BRASIL. Projeto de Lei nº 2.630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735>. Acesso em: 21 maio 2025.

BRASIL. Projeto de Lei nº 2.768/2022. Dispõe sobre a organização, o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro e dá outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2337417>. Acesso em: 24 maio 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 1.836.349/SP. Relator: Ministro Marco Aurélio Bellizze, Terceira Turma, julgado em 21 jun. 2022. Diário da Justiça Eletrônico, DJe de 24 jun. 2022. Disponível em: [https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencia=2181939&num\\_registro=201901346226&data=20220624&formato=PDF](https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencia=2181939&num_registro=201901346226&data=20220624&formato=PDF). Acesso em 24 maio 2025.

BRASIL. Superior Tribunal de Justiça. Recurso Especial nº 2092096, Civil, Consumidor e Processual Civil. Ação Indenizatória C/C Obrigação de Fazer. Relator: Ministra NANCY ANDRIGHI. Brasília, DF, 12 de dezembro de 2023. Brasília, 15 dez. 2023. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp?b=ACOR&livre=%28RESP.clas.+e+%40num%3D%222092096%22%29+ou+%28RESP.adj+%222092096%22%29.suce.&O=JT>. Acesso em: 03 abr. 2025.

BRASIL. Superior Tribunal de Justiça (STJ). Agravo em Recurso Especial 2.302.494/STJ. Relator: Ministro Raul Araújo. Diário da Justiça Eletrônico, Brasília, DF, 2023. Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp?preConsultaPP=&pesquisaAmigavel=+2302494&acao=pesquisar&novaConsulta=true&i=1&b=ACOR&livre=2302494&filtroPorOrgao=&filtroPorMinistro=&filtroPorNota=&data=&operador=e&thesaurus=JURIDICO&p=true&tp=P&processo=&classe=&uf=&relator=&dtpb=&dtpb1=&dtpb2=&dtde=&dtde1=&dtde2=&orgao=&ementa=&nota=&ref=>. Acesso em: 24 maio 2025.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 4906. Relator: Ministro Nunes Marques, julgado em 11 set. 2024. Diário da Justiça Eletrônico, s/n, divulgado em 23 out. 2024, publicado em 24 out. 2024. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur515682/false>. Acesso em: 24 maio 2025.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6.921 e 6.931. Relator: Ministro Alexandre de Moraes, julgado em 7 fev. 2024. A Constituição e o Supremo: Anotações do Supremo Tribunal Federal. Disponível em: <https://constituicao.stf.jus.br/dispositivo/cf-88-parte-1-titulo-7-capitulo-1-artigo-170>. Acesso em: 20 maio 2025.

BRASIL. Supremo Tribunal Federal. Agravo Regimental no Habeas Corpus 222.141/PR. Relator: Ministro Ricardo Lewandowski, Segunda Turma, julgado em 6 fev. 2024. Diário da Justiça Eletrônico, s/n, divulgado em 2 abr. 2024, publicado em 3 abr. 2024. Disponível em: <https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/HC222141.pdf>. Acesso em: 20 maio 2025.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental 449. Relator: Ministro Luiz Fux, julgado em 8 maio 2019. A Constituição e o Supremo: Anotações do Supremo Tribunal Federal. Disponível em: <https://constituicao.stf.jus.br/dispositivo/cf-88-parte-1-titulo-2-capitulo-1-artigo-5>. Acesso em: 20 maio 2025.

BRASIL. Supremo Tribunal Federal. Notícia: STF define parâmetros para responsabilização de plataformas por conteúdos de terceiros. Interpretação do Tribunal para norma do Marco Civil deve ser aplicada até que Congresso Nacional atualize a legislação. Disponível em: <https://noticias.stf.jus.br/postsnovicias/stf-define-parametros-para-responsabilizacao-de-plataformas-por-conteudos-de-terceiros/>. Acesso em: 27 jun. 2025.

BRASIL. Supremo Tribunal Federal. Notícia: Ministro Alexandre de Moraes dá prazo para Telegram cumprir integralmente determinações do STF. O ministro manteve a decisão que ordenou o bloqueio do aplicativo e afirmou que o cumprimento total é necessário para que seja suspensa a ordem de tirar o Telegram do ar. Petição 9.935 Distrito Federal. Disponível em: <https://noticias.stf.jus.br/postsnovicias/ministro-alexandre-de-moraes-da-prazo-para-telegram-cumprir-integralmente-determinacoes-do-stf/>. Acesso em 30 jun. 2025.

BRASIL. Supremo Tribunal Federal. Reclamação Constitucional nº 62.174/MG. Relator: Ministro Flávio Dino, Primeira Turma, julgado em 21 out. 2024. Diário da Justiça Eletrônico, DJe-s/n, divulgado em 24 out. 2024, publicado em 25 out. 2024. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur515982/false>. Acesso em: 21 maio 2025.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n. 1057258/MG. Relator: Min. Luiz Fux. Brasília, DF, julgado em 26 jun. 2025. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5217273>. Acesso em: 11 jul. 2025.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário n. 1037396/SP. Relator: Min. Dias Toffoli. Brasília, DF, julgado em 26 jun. 2025. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=5160549>. Acesso em: 11 jul. 2025

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário Com Agravo nº 660861. Relator: Ministro Luiz Fux. Brasília, DF, 22 de março de 2012. Brasília, 07 nov. 2012. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4155926>. Acesso em: 02 maio 2025.

BRASIL. Supremo Tribunal Federal. Segunda Turma. HC 222141 AgR. Relator: Min. Ricardo Lewandowski. Redator para o acórdão: Min. Gilmar Mendes. Julgado em 06/02/2024. Publicado no DJe em 03/04/2024. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur499454/false>. Acesso em: 22 abr. 2025.

BRASIL. Supremo Tribunal Federal (Plenário). Ação Direta de Inconstitucionalidade 3.510/DF. Relator: Min. Ayres Britto, 29 maio 2008. Diário de Justiça Eletrônico, Brasília, DF, 28 maio 2010. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur178396/false>. Acesso em: 22 abr. 2025.

BRASIL. Supremo Tribunal Federal (Plenário). Ação Direta de Inconstitucionalidade 5.783/BA. Relatora: Min. Rosa Weber, 06 set. 2023. Diário de Justiça Eletrônico, Brasília, DF, 14 nov. 2023. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur491014/false>. Acesso em: 22 abr. 2025.

BRASIL. Supremo Tribunal Federal (Plenário). Ação Direta de Inconstitucionalidade 6.649/DF. Relator: Min. Gilmar Mendes, 15 set. 2022. Diário de Justiça Eletrônico, Brasília, DF, 19 jun. 2023. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false>. Acesso em: 22 abr. 2025. Acesso em: 22 abr. 2025.

BRASIL. Supremo Tribunal Federal (Plenário). Recurso Extraordinário 1.054.110/SP. Repercussão Geral. Relator: Min. Roberto Barroso, 09 maio 2019. Diário de Justiça Eletrônico, Brasília, DF, 06 set. 2019. (Tema 967). Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur425705/false>. Acesso em: 22 abr. 2025.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 2.213 MC/DF. Relator: Ministro Marco Aurélio. Diário da Justiça Eletrônico, Brasília, DF, 2023. Disponível em: <https://www.conjur.com.br/wp-content/uploads/2023/09/adi-2213-stf-mst.pdf>. Acesso em: 20 maio 2025.

BRASIL. Terceira Câmara Cível do Tribunal de Justiça do Mato Grosso do Sul. Apelação Cível nº 0826377-93.2022.8.12.0001, Apelação em Ação de Rescisão Contratual e Indenização Por Dano Moral e Material. Relator: Juiz Alexandre Branco Pucci. Campo Grande, MS, 09 de maio de 2024. Campo Grande, 10 maio de 2024. Disponível em: <https://esaj.tjms.jus.br/cjsg/getArquivo.do?cdAcordao=1555281&cdForo=0>. Acesso em: 01 abr. 2025.

BRASIL. Tribunal de Justiça. Apelação Cível nº 1.017.172-48.2022.8.26.0007. Relator: Desembargador Luis Carlos de Barros, 20ª Câmara de Direito Privado. Diário da Justiça Eletrônico, São Paulo, 13 fev. 2025. Disponível em: <https://esaj.tjsp.jus.br/pastadigital/sg/abrirConferenciaDocumento.do>. Acesso em: 21 maio 2025.

BRASIL. Tribunal de Justiça de São Paulo. Apelação Cível nº 9126676-64.2005.8.26.0000. Relator: Desembargador Fortes Barbosa, 8ª Câmara de Direito Privado, julgado em 14 dez. 2011. Diário da Justiça Eletrônico, publicado em 16 dez. 2011. Acesso em: 20 maio 2025.

BRASIL. Tribunal de Justiça do Distrito Federal e dos Territórios. Acórdão nº 1.719.828. Apelação Cível nº 0702233-67.2022.8.07.0007. Relator: Desembargador Alfeu Machado, 6ª Turma Cível, julgado em 29 jun. 2023. Disponível em: <https://pje2i.tjdft.jus.br/consultap>. Acesso em: 21 maio 2025.

BORGES, Bruno de Moura. Desenvolvimento e Autonomia: O Brasil e a Tecnologia de Informação em Perspectiva Histórica Comparada. *Desigualdade & Diversidade*, n. 8, p. 77-100, 2011.

BUCCI, Maria Paula Dallari; COUTINHO, Diogo R. Arranjos jurídico-institucionais da política de inovação tecnológica: uma análise baseada na abordagem de direito e políticas públicas. *Inovação no Brasil: avanços e desafios jurídicos e institucionais*. São Paulo: Blucher, p. 313-340, 2017.

BUENO, Eric Fiuza; SANTOS, Marcelo Fonseca. Inteligência Artificial: Desafios Para Regulação Jurídica. *Direito & TI*, [S. l.], v. 1, n. 18, p. 112–139, 2024. Disponível em: <https://direitoeti.com.br/direitoeti/article/view/175>. Acesso em: 20 jun. 2025. <https://doi.org/10.63451/ti.v1i18.175>

CAMELO, Ana Paula et al. Soberania digital: para quê e para quem?: análise conceitual e política do conceito a partir do contexto brasileiro [recurso eletrônico]. São Paulo: FGV Direito SP, 2024. 38 p.

CAMPBELL-KELLY, Martin; ASPRAY, William; ENSMINGER, Nathan; YOST, Jeffrey R. *Computer: a history of the information machine*. 3. ed. New York: Westview Press, 2013.

CANONGIA, Claudia; JUNIOR, Raphael Mandarino. Segurança cibernética: o desafio da nova Sociedade da Informação. *Parcerias Estratégicas*, v. 14, n. 29, 2009.

CARVALHO, Lucas Borges de. Governo digital e direito administrativo: entre a burocracia, a confiança e a inovação. *Revista de Direito Administrativo*, [S. l.], v. 279, n. 3, p. 115–148, 2020. v279.2020.82959. Disponível em: <https://periodicos.fgv.br/rda/article/view/82959>. Acesso em: 20 jun. 2025. <https://doi.org/10.12660/rda>

CASELLA, Adriana Camargo Rodrigues. Proteção do "software" pelo direito do autor. *Revista da Faculdade de Direito, Universidade de São Paulo*, São Paulo, v. 81, p. 202-221, 1986.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2018.

CASTELLS, Manuel; CARDOSO, Gustavo. *A sociedade em rede: do conhecimento à acção política*. 2005. In: Conferência promovida pelo Presidente da República. 2015.

CERUZZI, Paul E. *A History of Modern Computing*. 2. ed. Cambridge, MA: MIT Press, 2003.

CUKIERMAN, H. L. A publicidade dos minicomputadores made in Brazil e a experiência da reserva de mercado dos anos 70/80. In: Anais do III Simposio de Historia de la Informática de América Latina y el Caribe. 2014. p. 17-28.

CUKIERMAN, Henrique Luiz; CASTRO, Rachel Gonçalves de; ALVES, Luiz Augusto da Silva. Os debates parlamentares das leis de informática (1984, 1991, 2001, 2004). In: I Simpósio De História Da Informática na ALC. Medellín, 2012.

DALLARI, Dalmo. O habeas data no sistema jurídico brasileiro. Revista da Faculdade de Direito, Universidade de São Paulo, v. 97, p. 239-253, 2002.  
<https://doi.org/10.11606/issn.2318-8235.v97i0p239-253>

D'ALMONTE, Edson Fernando; SANTOS, Alanna Oliveira. Regulamentação das plataformas digitais: entre a soberania digital e o transnacionalismo. In: E-Compós. 2024.

DATE, C. J. Introdução a Sistemas de Banco de Dados. 8. ed. Rio de Janeiro: Campus, 2003.

DEOCLECIANO, Pedro Rafael Malveira; LOBO, Julio César Matias; VIANA, Janile Lima. Uma análise crítica da atual posição do Supremo Tribunal Federal sobre o direito ao esquecimento. Revista Brasileira de Direito Civil, v. 31, n. 02, p. 203-203, 2022.

DONEDA, Danilo Cesar Maganhoto Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados. Revista dos Tribunais. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

ELEGIDO, Juan M. A ética da discriminação de preços. Business Ethics Quarterly, v. 21, n. 4, p. 633-660, 2011.

FIGUEIRÊDO, Simone de Sá Rosa; REIS, Elton Gomes. Poder e norma no ciberespaço. Revista Thesis Juris, v. 11, n. 2, p. 325-348, 2022. <https://doi.org/10.5585/rtj.v11i2.22684>

FILHO, Marco Aurélio Florêncio; LADEIRA, Fernando. Cidadania digital ou ditadura algorítmica? Contradições do mundo digitalizado e os desafios da regulação. Duc In Altum-Cadernos de Direito, v. 13, n. 31, 2021. <https://doi.org/10.22293/2179507x.v13i31.2176>

FRANCO, Fernanda Sathler Rocha. Regulação da Moderação De Conteúdo Digital e Principais Estratégias Jurídicas Brasileiras: Análise do Marco Civil da Internet, da Lei Geral de Proteção de Dados e do Projeto de Lei n. 2.630/20. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 10, n. 2, 2024.  
<https://doi.org/10.26668/IndexLawJournals/2526-0014/2024.v10i2.10903>

FRAZAO, Ana Oliveira; GOETTENAUER, Carlos. Algoritmos de precificação e direito concorrencial. Revista Eletrônica do Curso de Direito da UFSM, v. 17, n. 1, p. e40973-e40973, 2022.

FRAZÃO, Ana; OLIVA, Milena Donato; TEPEDINO, Gustavo. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. Thomson Reuters Brasil, 2020.

FREITAS, Luiz Otávio Rezende de; LUNARDI, Fabrício Castagna; CORREIA, Pedro Miguel Alves Ribeiro. Liberdade de expressão na era digital: novos intermediários e censura

por atores privados. *Revista de Investigações Constitucionais*, v. 11, n. 2, p. e262, 2024.  
<https://doi.org/10.5380/rinc.v11i2.89693>

GARCIA, Ana Cristina Bicharra. Ética e inteligência artificial. *Computação Brasil*, n. 43, p. 14-22, 2020.

GARCIA, Lara Rocha et al. *Lei Geral de Proteção de Dados (LGPD): guia de implantação*. Editora Blucher, 2020.

GROSSI, Bernardo Menicucci. *Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial*. Porto Alegre, RS: Editora Fi, 2020. E-book.

GUALDA, Diego de Lima. *Desafio Cultural da Proteção de Dados*. Disponível em:  
<https://aarb.org.br/desafio-cultural-da-protacao-de-dados/>. Acesso em 14 maio 2025.

HELENA, Silvia. A indústria de computadores: evolução das decisões governamentais. *Revista de Administração Pública*, v. 14, n. 4, p. 73-109, 1980.

HERMES, Pedro Henrique; LEAL, Rogério Gesta. A liberdade digital na Sociedade do Risco: perspectivas a partir da Proteção de Dados Pessoais. *Revista Eletrônica Direito & TI*, v. 1, n. 16, p. 158-185, 2023. <https://doi.org/10.1215/01636545-10637232>

IT Forum. *Dia da Informática: 6 empresas que marcaram a história da TI no Brasil*. Disponível em: <https://itforum.com.br/noticias/6-empresas-historia-informatica-brasil/>. Acesso em: 23 maio 2025.

JÚNIOR, José Eustáquio de Melo; OLIVEIRA, Gustavo Paschoal Teixeira de Castro. Contributos da Legística para a elaboração do marco legal da inteligência artificial no Brasil. *Revista de Informação Legislativa*, v. 60, n. 237, p. 99-114, 2023.  
[https://doi.org/10.70015/ril\\_v60\\_n237\\_p99](https://doi.org/10.70015/ril_v60_n237_p99)

JÚNIOR, Rubens José Kirk de Sanctis. A regulação das big techs no brasil: um imperativo democrático. *Revista da Seção Judiciária do Rio de Janeiro*, v. 28, n. 60, p. 74-100, 2024.  
<https://doi.org/10.30749/2177-8337.v28n60p74-100>

KLANN, Clarice. *Teoria Geral do Direito Digital*. Indaial: Uniasselvi, 2020.

LAUDON, Kenneth C.; LAUDON, Jane P. *Sistemas de Informações Gerenciais*. 11. ed. São Paulo: Pearson Education do Brasil, 2014.

LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. Nova Iorque: Basic Books, 1999.

LOPES, Maria Margaret. *A política brasileira de informática: 1970-1984*. Dissertação (Mestrado em Ciência Política) - Universidade de São Paulo, São Paulo, 1986.

MARCELINO, Gileno Fernandes. A indústria nacional de computadores. *Revista de Administração de Empresas*, São Paulo, v. 43, n. 2, p. 8-20, 2003. Disponível em:  
<https://www.revistas.usp.br/rausp/article/download/166948/159505/393477>. Acesso em: 12 maio 2025.

MARTINS, Flavio. Curso de Direito Constitucional. 8. ed. São Paulo: Saraiva, 2024.

MAXIM, Bruce R.; PRESSMAN, Roger S. Engenharia de Software: uma abordagem profissional. Porto Alegre:[sn], 2021.

MENDES, Gilmar Ferreira. Roberto Campos: o Constituinte profeta. Revista de Informação Legislativa: RIL, Brasília, DF, v. 59, n. 236, p. 11-27, out./dez. 2022. Disponível em: [https://www12.senado.leg.br/ril/edicoes/59/236/ril\\_v59\\_n236\\_p11](https://www12.senado.leg.br/ril/edicoes/59/236/ril_v59_n236_p11). Acesso em 7 de abr. de 2025. [https://doi.org/10.70015/ril\\_v59\\_n236\\_p11](https://doi.org/10.70015/ril_v59_n236_p11)

MIGUEL, Henrique. Tecnologia da Informação: Legislação Brasileira - Atualização. Brasília: Ministério da Ciência, Tecnologia e Inovações (MCTI), 2024. Disponível em: <https://www.gov.br/mcti/ptbr/centrais-de-conteudo/publicacoes-mcti/tecnologia-da-informacao-legislacao-atualizada/tecnologia-dainformacao-legislacao-atualizada>. Acesso em: 15 maio 2025.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO - MCTI; CENTRO DE GESTÃO E ESTUDOS ESTRATÉGICOS - CGEE. IA para o bem de todos; Plano Brasileiro de Inteligência Artificial. Brasília, DF: MCTI;CGEE, 2025. 104p.

MOREIRA, José Carlos Barbosa. O habeas data brasileiro e sua lei regulamentadora. Revista de Direito Administrativo, v. 211, p. 47-63, 1998. <https://doi.org/10.12660/rda.v211.1998.47125>

MOREIRA, Nelson Camatta; MOREIRA JÚNIOR, Ronaldo Fêlix. A construção do constitucionalismo digital na era da desinformação: o caso Cambridge Analytica e seu impacto no ecossistema constitucional. Revista de Informação Legislativa, 2023.

MÜLLER, William; SILVEIRAS, Raphael. A Evolução e a Regulamentação da Inteligência Artificial no Brasil. Revista InterCiência-IMES Catanduva, v. 1, n. 11, p. 2-2, 2023.

NETO, Elias Jacob de Menezes et al. Accountability, transparência e assimetria das relações de visibilidade virtuais: análise dos aspectos antidemocráticos das novas tecnologias da informação e comunicação a partir da ideia de filtro bolha. Revista Direito, Estado e Sociedade, n. 53, 2018.

O'KANE, Philip; SEZER, Sakir; CARLIN, Domhnall. Evolução do ransomware. Iet Networks, v. 7, n. 5, p. 321-327, 2018. <https://doi.org/10.1049/iet-net.2017.0207>

PEREIRA, L.; MARINHO, MGSMC. O cérebro eletrônico do IBGE: análise sobre os impactos da importação de um computador eletrônico para a realização do Censo de 1960. Anais III SHIALC, p. 1-8, 2014.

PEREIRA, Adriano; SIMONETTO, Eugênio de Oliveira. Indústria 4.0: conceitos e perspectivas para o Brasil. Revista da Universidade Vale do Rio Verde, v. 16, n. 1, 2018.

PINHEIRO, Patrícia Peck. Direito Digital. 8. ed. São Paulo: Saraiva, 2017.



PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: comentários à Lei n. 13.709/2018-LGPD. Saraiva Educação SA, 2018.

PRESSMAN, Roger S.; MAXIM, Bruce R. Engenharia de software-9. McGraw Hill Brasil, 2021.

RODRIGUES, Silvia Helena. Como a defesa de uma indústria brasileira de informática ganhou as páginas da grande imprensa. In: TAROUCO, Liane Margarida Rockenbach; MUSSE, Jussara Issa. Memórias do V Simpósio de História da Informática na América Latina e Caribe. Rio de Janeiro: UFRJ, 2018.

ROMÃO, Carolina Brasil et al. A indústria dos jogos eletrônicos: novas tecnologias, propriedade intelectual e cenário mundial e brasileiro. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência, v. 5, n. 1, p. 1-20, 2019.  
<https://doi.org/10.26668/IndexLawJournals/2526-0014/2019.v5i1.5394>

SALEN, Katie; ZIMMERMAN, Eric. Rules of Play: Game Design Fundamentals. Cambridge: MIT Press, 2004.

SANTOS, Gabrielly Cordeiro dos; COELHO, Ivana Lara Ribeiro; BERNARDES, Rochele Juliane Lima Firmeza. Entre a diversão e a ruína: a influência das apostas online/bets no endividamento excessivo do brasileiro. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 11, n. 4, p. 3396-3420, 2025. <https://doi.org/10.51891/rease.v11i4.18903>

SANTOS, Givanildo de Jesus, et al. Análise da política brasileira de proteção da propriedade intelectual para softwares e invenção implementada por computador (IIC). OBSERVATÓRIO DE LA ECONOMÍA LATINOAMERICANA, v. 21, n. 7, p. 6239-6262, 2023.  
<https://doi.org/10.55905/oelv21n7-22>

SANTOS, Regiane Martins dos; CARVALHO, Adriana Cristina França Leite de. Comentários à Lei Geral de Proteção de Dados. São Paulo: OAB, 2020.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988. Direitos Fundamentais & Justiça, 2020.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos Jusfilosóficos e Âmbito de Proteção do Direito Fundamental à Proteção de Dados Pessoais. Direito Público, [S.l.], v. 17, n. 93, p. 34-57, 2020. Disponível em:  
<https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315>. Acesso em: 22 jun. 2025. <https://doi.org/10.13110/antipodes.34.1.0057>

SCHMIDT, Albano Francisco; AMARAL, Luise; COUTO, Vanessa Ribeiro. Marco Legal dos Games: análise exploratória do cenário econômico dos jogos digitais e sua relevância para a economia brasileira. 2024.

SETO, Kenzo Soares. A regulação e governança das plataformas digitais: uma revisão sistemática de literatura. Revista Eptic Online, v. 23, n. 3, 2021.

SOUZA, Carlos Diego Peixoto de. Limitação ao direito fundamental à proteção de dados pessoais (Artigo 5.º, LXXIX): da constitucionalidade do substitutivo ao Projeto de Lei n.º

118/2021. Jus Scriptum's International Journal of Law, v. 8, n. 3-4, p. 178-224, 2023.  
<https://doi.org/10.29327/238407.8.3-7>

TAVARES, André Ramos. Ciência e tecnologia na Constituição. Revista de Informação Legislativa. Brasília: Senado Federal, a, v. 44, p. 7, 2007.

TECNOBLOG. Relembrando a proteção à indústria de PCs no Brasil - e os custos de limitar importações. Tecnoblog, [s. l.], 2019. Disponível em:  
<https://tecnoblog.net/especiais/relembrando-a-protecao-a-industria-de-pcs-no-brasil-e-os-custos-de-limitar-importacoes/>. 12 maio 2025.

TURBAN, Efraim; VOLONINO, Linda; WOOD, Gregory. Tecnologia da Informação para Gestão. 9. ed. Porto Alegre: Bookman, 2013.

VALENTE, Cristina de Melo. Computadores e Educação: momentos iniciais desta relação no Brasil. iSys-Brazilian Journal of Information Systems, v. 10, n. 2, p. 193-219, 2017.  
<https://doi.org/10.5753/isys.2017.341>

VARGAS, Milton. História da Informática no Brasil. Rio de Janeiro: Campus, 1996.

VIANNA, Marcelo; ZEFERINO, PRISCILA Yasmin da Rocha; CUNHA, Laura Castro da. “O futuro nunca esteve tão presente em sua vida”: o microcomputador na sociedade brasileira através da revista Micro Sistemas (1981-1983). MoExp-Mostra de Ensino, Extensão e Pesquisa do Campus Osório, v. 1, n. 1, p. 1-1, 2018.

VIEGAS, Cláudia Mara de Almeida Rabelo. Proteção jurídica do software. JusBrasil, 2020. Disponível em: <https://www.jusbrasil.com.br/artigos/propriedade-industrial-protecao-juridica-do-software/760054078>. Acesso em: 12 maio 2025.

WORLD INTELLECTUAL PROPERTY ORGANIZATION (WIPO). Software and Business Methods. Genebra: WIPO, 2023. Disponível em: <https://www.wipo.int/portal/en/index.html>. Acesso em: 24 maio 2025.

ZENDLE, David; MEYER, Rachel; OVER, Harriet. Adolescentes e loot boxes: Ligações com jogo problemático e motivações para compra. Royal Society open science, v. 6, n. 6, p. 190049, 2019

## 9 ANEXOS

**Tabela 2** - Quadro da evolução normativa

ANO	NORMA	CATEGORIA
1960	Decreto nº 47.701	Regulamentação de <i>hardware</i>
1967	Portaria nº 322	Regulamentação de <i>hardware</i>
1967	Decreto-Lei nº 200	Estrutura administrativa
1972	Decreto nº 70.370	Regulamentação de <i>hardware</i>
1972	Decreto-Lei nº 1.209	Regulamentação de <i>software</i>
1973	Lei nº 5.988	Regulamentação de <i>software</i>
1975	Portaria interministerial nº 10/75	Regulamentação de <i>hardware</i>
1976	Portaria nº 291	Regulamentação de <i>hardware</i>
1979	Portaria nº 361	Regulamentação de <i>hardware</i>
1979	Decreto nº 84.067	Regulamentação de <i>hardware</i>
1984	Lei nº 7.232	Regulamentação de <i>software</i>
1987	Lei nº 7.646	Regulamentação de <i>software</i>
1990	Código de Defesa do Consumidor	Proteção de dados
1996	Lei nº 9.279	Regulamentação de <i>hardware</i>
1996	Lei nº 9.296	Proteção de dados
1997	Lei nº 9.507	Proteção de dados
1998	Lei nº 9.609	Regulamentação de <i>software</i>

1998	Lei nº 9.610	Regulamentação de <i>software</i>
2001	Medidas Provisórias nº 2.200-2	Regulamentação da internet
2004	Lei nº 10.973	Política de Inovação
2011	Lei nº 12.527	Proteção de dados
2012	Lei nº 12.737	Segurança da informação
2014	Lei nº 12.965	Regulamentação da internet
2018	Lei nº 13.709	Proteção de dados
2018	Lei nº 13.756	Regulamentação de jogos eletrônicos
2018	Decreto nº 9.637	Segurança da informação
2020	Decreto nº 10.222	Segurança da informação
2020	PL nº 21	Regulamentação de IA
2022	EC nº 115	Proteção de dados
2023	Lei nº 14.790	Regulamentação de apostas/jogos eletrônicos
2023	Decreto nº 11.856	Regulamentação da LGPD
2023	PL nº 2338/2023 (em tramitação)	Regulamentação de IA
2024	Lei nº 14.846	Crimes cibernéticos
2024	Lei nº 14.852	Regulamentação de jogos eletrônicos

**Tabela 3** - Agrupamento das normas por assuntos

CATEGORIA	NORMAS
Regulamentação de <i>hardware</i>	<p>Decreto nº 47.701/1960</p> <p>Portaria nº 322/1967</p> <p>Decreto nº 70.370/1972</p> <p>Portaria interministerial nº 10/1975</p> <p>Portaria nº 291/1976</p> <p>Portaria nº 361/1979</p> <p>Decreto nº 84.067/1979</p> <p>Lei nº 9.279/1996</p>
Regulamentação de <i>software</i>	<p>Decreto-Lei nº 1.209/1972</p> <p>Lei nº 5.988/1973</p> <p>Lei nº 7.232/1984</p> <p>Lei nº 7.646/1987</p> <p>Lei nº 9.609/1998</p> <p>Lei nº 9.610/1998</p>
	<p>Constituição Federal de 1988</p> <p>Código de Defesa do Consumidor (1990)</p> <p>Lei nº 9.296/1996</p> <p>Lei nº 9.507/1997</p>

Proteção de dados	Lei nº 12.527/2011 Lei nº 12.965/2014 Lei nº 13.709/2018 EC nº 115/2022 Decreto nº 11.856/2024
Segurança cibernética	Lei nº 12.737/2012 Decreto nº 9.637/2018 Decreto nº 10.222/2020 Lei nº 14.846/2024
Regulamentação da internet	Medidas Provisórias nº 2.200-2/2001 Lei nº 12.965/2014
Regulamentação de jogos eletrônicos	Lei nº 13.756/2018 Lei nº 14.790/2023 Lei nº 14.852/2024
Regulamentação de IA	PL nº 21/2020 PL nº 2338/2023
Regulamentação de jogos eletrônicos	Lei nº 13.756/2018 Lei nº 14.790/2023 Lei nº 14.852/2024
Estrutura administrativa	Decreto-Lei nº 200/1967 Lei nº 10.973/2004

**Tabela 4 - Eventos – Linha Evolutiva**

<b>DÉCADA</b>	<b>EVENTOS E NORMAS</b>	<b>CATEGORIA</b>
1950	Importação do primeiro computador no Brasil para o setor público.	<i>hardware</i>
	Início da informatização da sociedade brasileira.	
1960	Decreto nº 47.701/1960: Organização dos serviços de processamento de dados na administração federal.	Regulamentação de <i>hardware</i>
	Entrada de empresas multinacionais no mercado brasileiro, como a IBM.	
	Portaria nº 322/1967: Criação do Grupo Executivo para o Desenvolvimento da Indústria de Computadores Eletrônicos (GEDICE).	Regulamentação de <i>hardware</i>
	Decreto-Lei nº 200/1967: Organização da Administração Federal direta e indireta.	Outros
	Implementação de políticas protecionistas para desenvolver a indústria de computadores doméstica	
	Decreto nº 70.370/1972: Criação da Comissão de Coordenação das Atividades de Processamento Eletrônico (CAPRE)	Regulamentação de <i>hardware</i>

1970	Decreto-Lei nº 1.209/1972: Incentivos fiscais para empresas que investissem na produção de equipamentos e <i>softwares</i> de informática.	Regulamentação de <i>software</i>
	Lei nº 5.988/1973: Lei de Direitos Autorais (inicialmente utilizada para proteção de <i>softwares</i> ).	
	Portaria interministerial nº 10/75: Normas para concessão de incentivos fiscais à produção de componentes eletrônicos.	Regulamentação de <i>hardware</i>
	Portaria nº 291/1976: Normas para importação de equipamentos e <i>softwares</i> de informática.	
	Portaria nº 361/1979: Atualização das normas de importação.	
	Decreto nº 84.067/1979: Criação da Secretaria Especial de Informática (SEI).	
1980	Lei nº 7.232/1984: Instituição do regime jurídico de reserva de mercado de informática.	Regulamentação de <i>software</i>
	Lei nº 7.646/1987: Primeira lei específica para a proteção de <i>software</i> no Brasil.	
	Popularização dos microcomputadores e início da "Revolução do PC".	
	Código de Defesa do Consumidor (1990): Disposições sobre proteção de dados em relações de consumo.	Proteção de dados
	Lei nº 9.279/1996: Lei da Propriedade Industrial (LPI), utilizada para proteção de <i>hardware</i> .	Regulamentação de <i>hardware</i>
	Lei nº 9.296/1996: Lei das Interceptações Telefônicas, abordando a inviolabilidade do sigilo das comunicações.	



1990	Lei nº 9.507/1997: Lei do Habeas Data, regulamentando o direito de acesso a informações pessoais.	Proteção de dados
	Lei nº 9.609/1998: Segunda Lei de <i>Software</i> , consolidando a proteção do <i>software</i> por direitos autorais.	Regulamentação de <i>software</i>
	Lei nº 9.610/1998: Atualização da Lei de Direitos Autorais, incorporando dispositivos sobre proteção de <i>software</i> .	
	Ascensão da internet e da era digital, impulsionando a demanda por <i>softwares</i> .	
2000	Medidas Provisórias nº 2.200-2/2001: Instituição da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).	Regulamentação da internet
	Lei nº 10.973/2004: Lei de Inovação, incentivando a pesquisa e o desenvolvimento tecnológico.	Outros
2010	Lei nº 12.527/2011: Lei de Acesso à Informação (LAI), garantindo o acesso a informações públicas.	Proteção de dados
	Lei nº 12.737/2012: Lei Carolina Dieckmann, tipificando crimes cibernéticos.	Segurança da informação
	Lei nº 12.965/2014: Marco Civil da Internet, estabelecendo princípios e garantias para o uso da internet.	Regulamentação da internet
	PL nº 21/2020: Projeto de Lei que busca estabelecer o Marco Legal da Inteligência Artificial.	Regulamentação de IA
	Decreto nº 9.637/2018: Instituição da Política Nacional de Segurança da Informação (PNSI).	Segurança da informação
	Decreto nº 10.222/2020: Aprovação da Estratégia Nacional de Segurança Cibernética ( <i>E-Ciber</i> ).	

2020	Lei nº 13.709/2018: Lei Geral de Proteção de Dados (LGPD), regulamentando a proteção de dados pessoais.	Proteção de dados
	Lei nº 13.756/2018: Lei de incentivo aos jogos eletrônicos, buscando o desenvolvimento da indústria nacional.	Regulamentação de jogos eletrônicos
	EC nº 115/2022: Alteração do artigo 5º da Constituição Federal para incluir o direito à proteção de dados pessoais.	Proteção de dados
	Lei nº 14.790/2023: Lei que dispõe sobre as apostas de quota fixa.	Regulamentação de jogos eletrônicos
	Lei nº 14.852/2024: Marco Legal dos Jogos Eletrônicos, criando um ambiente regulatório favorável à indústria.	