

UNILEÃO
CENTRO UNIVERSITÁRIO DOUTOR LEÃO SAMPAIO
CURSO DE GRADUAÇÃO EM DIREITO

JENIFER BATISTA DE SOUZA

A RELAÇÃO DAS BIGTECHS E A PROTEÇÃO DE DADOS: A influência da inteligência
artificial.

JUAZEIRO DO NORTE-CE
2025

JENIFER BATISTA DE SOUZA

A RELAÇÃO DAS BIGTECHS E A PROTEÇÃO DE DADOS: A influência da inteligência artificial.

Trabalho de Conclusão de Curso – *Artigo Científico*, apresentado à Coordenação do Curso de Graduação em Direito do Centro Universitário Doutor Leão Sampaio, em cumprimento às exigências para a obtenção do grau de Bacharel.

Orientador: Abreviação da Titulação do Orientador e o Nome Completo do Orientador, Esp. Francisco Gledison Lima Araujo.

JENIFER BATISTA DE SOUZA

A RELAÇÃO DAS BIGTECHS E A PROTEÇÃO DE DADOS: A influência da inteligência artificial.

Este exemplar corresponde à redação final aprovada do Trabalho de Conclusão de Curso de JENIFER BATISTA DE SOUZA

Data da Apresentação 05/11/2025

BANCA EXAMINADORA

Orientador: ME. Francisco Gledison Lima Araujo

Membro: ESP. André Carvalho Barreto – UNILEÃO

Membro: DR. José Eduardo Carvalho de Lima - UNILEÃO

JUAZEIRO DO NORTE-CE
2025

A RELAÇÃO DAS BIGTECHS E A PROTEÇÃO DE DADOS: A influência da inteligência artificial.

Jenifer Batista de Souza¹
Francisco Gledison Lima Araujo²

RESUMO

O presente trabalho visa analisar a relação das Big techs e startups frente ao uso da inteligência artificial (IA) quanto a proteção de dados dos usuários, analisando como a Lei Geral de Proteção de Dados (LGPD), Marco Civil da Internet (MCI) e a Lei Carolina Dieckmann (Lei nº 12.737/2012) trabalham em conjunto assegurando que tais dados sejam coletados, armazenados e compartilhados de modo seguro e transparente. O estudo analisa como a inteligência artificial pode ser eficiente ao realizar tarefas de alta complexidade, observando sua automação diante da alta demanda do serviço ofertado, bem como pode ser maléfica se usada de maneira incorreta. Trata-se de uma pesquisa básica estratégica, exploratória, qualitativa, realizada por meio de revisão de literatura. Pretende-se, ao final analisar como a inteligência artificial atua cooperando para o trabalho das empresas e quais possíveis porporções ela pode adquirir.

Palavras Chave: Inteligência artificial, LGPD, MCI, Big Tech, Empresa

1 INTRODUÇÃO

Nos últimos anos, a inteligência artificial emergiu como uma das tecnologias mais transformadoras no âmbito empresarial, principalmente em big techs e startups a qual têm impulsionado o avanço digital em diversos setores. A implementação da IA tem possibilitado a automação e otimização de tarefas, em especial aquelas repetitivas e de alta complexidade, refletindo diretamente na eficiência das atividades empresariais. Entretanto, paralelamente a esses avanços, cresce a preocupação com a proteção dos dados pessoais, tendo em vista o aumento exponencial do volume de informações sensíveis processados por essas tecnologias.

¹Graduando do Curso de Direito do Centro Universitário Doutor Leão Sampaio/Unileão-jeniferbatistta@gmail.com

² Professor do Centro Universitário Doutor Leão Sampaio/UNILEÃO, Mestrando em Direito Constitucional – Unifieo – SP franciscogledison@leaosampaio.edu.br

No Brasil, este cenário é regulado por legislações específicas que visam garantir a privacidade e a segurança dos dados, destacando-se a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet (MCI) e a Lei Carolina Dieckmann (Lei nº 12.737/2021). Estas normativas estabelecem bases para a coleta, armazenamento e compartilhamento seguro e transparente dos dados dos usuários, buscando mitigar riscos e garantir direitos fundamentais no ambiente digital.

Dessa forma, este trabalho busca analisar como a inteligência artificial, especialmente em big techs e startups, interage com o contexto jurídico da proteção de dados, apresentando os benefícios, desafios e limitações impostas por esse cenário tecnológico que está em constante evolução.

A relevância do presente estudo reside no fato de que embora as tecnologias de IA estejam cada vez mais incorporadas ao cotidiano empresarial e social, as estruturas legislativas ainda enfrentam desafios para se adaptar rapidamente às inovações, o que pode resultar em vulnerabilidades no tratamento dos dados pessoais dos usuários. Além disso, o impacto da IA na eficiência organizacional deve ser avaliado com cautela para que os avanços tecnológicos não comprometam a privacidade e a segurança das informações.

Portanto, analisar a relação das big techs com a proteção de dados no contexto da IA é essencial para entender os mecanismos jurídicos existentes e apontar caminhos para o desenvolvimento de políticas práticas para que equilibrem inovação tecnológica com o respeito aos direitos dos cidadãos.

O objetivo geral deste estudo é analisar a relação entre big techs e proteção de dados, enfocando a influência da inteligência artificial na gestão e segurança das informações pessoais. Como objetivos específicos é necessário examinar o papel das big techs no tratamento de dados sensíveis com o uso da IA identificando os principais dispositivos legais brasileiros que regulam a proteção de dados pessoais, avaliando vantagens e riscos da utilização de IA no processamento de informações, e discutir os desafios éticos e jurídicos enfrentados pelas empresas perante as legislações vigentes. Este trabalho caracteriza-se como uma pesquisa básica, exploratória e qualitativa, realizada por meio de revisão bibliográfica e documental.

Foram consultadas obras especializadas, artigos acadêmicos, legislações pertinentes e relatórios técnicos relacionados às big techs, inteligência artificial e proteção de dados. A abordagem qualitativa permitiu compreender os aspectos legais e tecnológicos envolvidos, bem como interpretar criticamente os benefícios e limitações da IA no contexto jurídico brasileiro.

2 DESENVOLVIMENTO

2.1 METODOLOGIA

A metodologia empregada na construção deste artigo fundamenta-se em uma pesquisa qualitativa de natureza exploratória, pautada essencialmente na revisão bibliográfica e documental. O desenvolvimento do estudo iniciou-se com a seleção de fontes especializadas, englobando livros, artigos acadêmicos, legislações vigentes e relatórios técnicos, com foco nos temas: inteligência artificial, governança corporativa, proteção de dados pessoais no contexto regulatório brasileiro e internacional.

Inicialmente, procedeu-se a uma ampla leitura e análise crítica da literatura, com a identificação de conceitos-chave, desafios e boas práticas relacionadas à implementação e governança da IA no ambiente das big techs e startups. A partir dessa base teórica, foram exploradas as principais normativas aplicáveis, tais como a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet e a Lei Carolina Dieckmann, avaliando sua adequação e aplicação prática frente às inovações tecnológicas.

Além disso, foram incorporados estudos de casos recentes, notícias e documentos oficiais para ilustrar as implicações reais das práticas de governança da IA e os desafios enfrentados no Brasil, dando assim uma dimensão aplicada e atualizada à pesquisa. Houve, ainda, uma análise crítica que buscou traçar conexões entre aspectos técnicos, éticos e jurídicos da proteção de dados em IA enfatizando a necessidade de transparência, ética e responsabilidade corporativa.

Ao final, o método utilizado visou proporcionar um entendimento aprofundado e contextualizados do tema, permitindo não apenas mapear o estado da arte em governança de IA, mas também identificar lacunas regulatórias e recomendar caminhos para um uso mais ético e seguro dessa tecnologia, alinhando às exigências legais e às expectativas sociais contemporâneas.

Essa abordagem metodológica buscou garantir que o artigo fosse construído com rigor acadêmico, relevância prática e clareza conceitual, com a finalidade de possibilitar que os leitores compreendam os múltiplos desafios e perspectivas que envolvam a governança da inteligência artificial nas big techs e startups no Brasil.

2.2 REFERENCIAL TEÓRICO

A inteligência artificial tem sido definida como um conjunto de técnicas computacionais capazes de simular a capacidade humana de raciocínio, aprendizado e tomada de decisão. Segundo Russell e Norvig (2021), a IA abrange desde algoritmos simples até complexos sistemas capazes de processar dados em grande escala para fornecer soluções em tempo real, sendo amplamente aplicada em empresas de tecnologia que buscam otimizar processos e explorar novos modelos de negócios.

Big techs, gigantes do setor tecnológico como Google, Amazon, Facebook, Apple e Microsoft, são protagonistas na adoção e desenvolvimento da IA. Essas empresas manejam volumes massivos de dados pessoais e sensíveis, utilizados para alimentar sistemas inteligentes que aprimoram serviços, publicidade direcionada, e-commerce e análise preditiva (Zuboff, 2019). Entretanto, esse tratamento intensivo de dados levanta questões cruciais sobre segurança, privacidade e ética.

A proteção de dados pessoais, por sua vez, ganhou destaque mundial com o crescimento exponencial da digitalização da informação. No Brasil, a Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, representa um marco regulatório para assegurar direitos dos titulares de dados e impor obrigações às organizações. A LGPD define princípios fundamentais, como a finalidade, necessidade, transparência, segurança e responsabilização, que regulam o tratamento de dados pessoais, inclusive pela IA (Brasil, 2018).

O Marco Civil da Internet, constituído pela Lei nº 12.965/2014, complementa essa proteção ao garantir direitos à privacidade e à proteção dos dados pessoais no ambiente digital, além de estabelecer princípios para o uso da internet no Brasil. Já a Lei Carolina Dieckmann (Lei nº 12.737/2012) configura crimes informáticos, incluindo invasão de dispositivos eletrônicos para obtenção indevida de dados, reforçando assim a proteção jurídica contra abusos digitais (TEXEIRA, 2024).

No contexto da IA aplicada por big techs e startups, o big data desempenha papel essencial. Ele envolve a coleta, armazenamento e análise de enormes conjuntos de dados que alimentam os algoritmos inteligentes, gerando insights que impulsionam não somente a inovação, mas também ampliam os riscos de exposição e uso inadequado das informações (PECK, 2021). Assim, o equilíbrio entre inovação e a proteção dos direitos fundamentais torna-se um desafio crescente.

Os desafios éticos da IA também são destacados por autores como PECK (2021), que apontam que, sem diretrizes claras, a automatização e decisões algorítmicas podem perpetuar preconceitos, discriminação e opacidade, agravando vulnerabilidades sociais. Em consequência, além das normas legais, cresce a importância de políticas corporativas

transparentes e mecanismos de governança responsáveis no uso da IA.

2.3 O PAPEL DAS BIG TECHS NO TRATAMENTO DE DADOS COM IA

As big techs exercem papel central no ecossistema digital contemporâneo, dado o seu controle sobre grandes volumes de dados pessoais utilizados para alimentar sistemas de inteligência artificial. Essas empresas aplicam algoritmos de aprendizado de máquina para melhorar serviços, personalizar experiências e otimizar processos internos. Como destaca Viviane Sá, gerente de privacidade e DPO, a IA tem potencial para automatizar monitoramento e auditoria de dados em tempo real, aumentando eficiência e reduzindo erros humanos na gestão da conformidade regulatória (PECK, 2021).

Esses avanços tecnológicos, no entanto, também aumentam o risco de violações de privacidade e exposição inadequada de informações sensíveis, sendo essencial que as big techs estabeleçam políticas rigorosas de governança e transparência acerca do uso dos dados. A aplicação inadequada da IA pode reduzir custos e elevar a precisão das operações, promovendo melhorias significativas na tomada de decisões empresariais.

No Brasil, o arcabouço jurídico voltado para a proteção dos dados pessoais contempla sobretudo a LGPD, que estabelece princípios fundamentais como a finalidade e transparência no tratamento das informações prestadas. O Marco Civil da Internet integra o regime ao garantir direitos no ambiente digital e regulamentar as responsabilidades dos provedores de internet. A Lei Carolina Dieckmann trouxe uma resposta penal contra violações, como a invasão de dispositivos e divulgação não autorizada de dados e imagens (Brasil, 2018; Gomes et al., 2020).

A recente inclusão do direito à proteção de dados como direito fundamental na Constituição Federal reforça a importância da proteção jurídica eficaz num contexto de crescente digitalização (Peck, 2021). Contudo, a efetividade prática dessas normas ainda enfrenta desafios, principalmente diante da rápida evolução tecnológica das big techs e das complexidades inerentes ao uso da IA.

Os benefícios da IA no tratamento de dados pessoais incluem a capacidade de identificar automaticamente padrões incomuns, prevenir fraudes e monitorar conforme as normas de privacidade, além de aprimorar a segurança digital com mecanismos como autenticação biométrica e análise comportamental, a IA permite uma análise mais rápida e precisa, facilitando decisões estratégicas mais efetivas nas organizações.

Por outro lado, os riscos tornam-se evidentes na possibilidade de falhas nos sistemas, como falsos positivos na detecção de fraudes, e a exposição não autorizada de dados sensíveis

por vulnerabilidades, o que pode gerar supervisão humana adequada pode também comprometer direitos fundamentais, o que tornará imprescindível a adoção de controles rigorosos, (TEIXEIRA, 2024).

2.3 DESAFIOS ÉTICOS E JURÍDICOS NA GOVERNANÇA DA IA

Além dos desafios técnicos, a ética na inteligência artificial é um dos temas centrais na discussão sobre a proteção de dados pessoais, da a automação das decisões algorítmicas pode exacerbar preconceitos existentes, reduzir a transparência e dificultar a atribuição de responsabilidades por possíveis abusos. Um desafio fundamental é o “viés algorítmico”, em que sistemas treinados em dados históricos tendenciosos replicam ou ampliam disparidades sociais, gerando discriminação e concessão de crédito (Mindtek, 2025). Autores brasileiros como Dora Kaufman apontam que esses vieses sociais e éticos exigem estratégias regulatórias rigorosas para evitar que a tecnologia reproduza injustiças sociais preexistentes (KAUFMAN, 2023).

Para mitigar esses riscos, há um consenso crescente sobre a necessidade da governança responsável da IA, que envolve implementação de práticas como anonimização e criptografia dos dados pessoais. A anonimização remove informações identificáveis para que os dados não possam ser rastreados a um indivíduo específico, enquanto a minimização limita a coleta apenas ao que é estritamente preciso para o propósito definido (YSSY, 2023; Serpro, 2024). A criptografia assegura que os dados estejam protegidos tanto em trânsito quanto em repouso, evitando acessos não autorizados (Templo.pro, 2024). Ademais, auditorias independentes e regulares dos sistemas de IA são fundamentais para garantir a conformidade legal e a ética, permitindo avaliar a existência de falhas e vieses (IBM, 2024; GrantThornton, 2025). No Brasil, pesquisadores como Ana Frazão destacam a importância dessas medidas integradas em protocolos de governança para garantir a segurança e confiança na IA (FRAZÃO. 2023).

Transparência emerge como pilar essencial para a governança ética da IA. Tornar explicável a lógica, funcionamento e base das decisões algorítmicas – o conceito de IA explicável (XAI) – é crucial para construção de confiança entre usuários e desenvolvedores. Isto não apenas promove a compreensão pública sobre o impacto da tecnologia, mas também facilita a responsabilização em caso de decisões equivocadas ou prejudiciais (Serpro, 2024; Geotab, 2025). A falta de transparência, ou a chamada “caixa preta” da IA, pode intensificar inseguranças e desconfianças, prejudicando a adoção ética da tecnologia (IBM, 2024). Pesquisadores brasileiros como Alexandre Zavaglia ressaltam que a opacidade de algoritmos é

uma das maiores barreiras para a regulamentação eficaz e para a proteção dos direitos dos cidadãos no meio digital (ZAVAGLIA, 2023).

No âmbito jurídico, o Brasil ainda se encontra em estágio inicial na elaboração de regulamentações específicas para IA, apesar de iniciativas como o projeto de lei PL 21/2020, que visa estabelecer princípios e diretrizes para seu uso responsável (Revista Tópicos, 2025). Enquanto isso, normas vigentes como a LGPD e o MCI, são aplicadas para regular o tratamento de dados que sustentam esses sistemas. A falta de regras claras sobre as responsabilidades civil em decisões automatizadas cria desafios na tutela de direitos dos cidadãos (Assis e Mendes, 2018). Edson Santos, em suas análises jurídicas, destaca a urgência em consolidar marcos normativos que contribuam para responsabilizar de modo objetivo e específico os danos causados por IA (SANTOS, 2024).

A governança ética da IA em big techs e startups depende também do compromisso corporativo com práticas responsáveis, que incorporam mecanismos de controle de acesso rigoroso, auditorias de segurança e treinamentos acessíveis para equipes técnicas e decisórias (Templo.pro, 2024). A atualização desses processos, acompanhando o avanço tecnológico e as descobertas em segurança digital, é vital para evitar brechas e prejuízos (Galicia Educação, 2024). Assim, Marina Feferbaum aponta que a capacitação contínua e a conscientização ética dos envolvidos são essenciais para a efetividade e legitimidade da governança (FERFERBAUM, 2023).

Por último, debates internacionais liderados por organizações como UNESCO, Comissão Europeia e Fórum Econômico Mundial, destacam princípios que devem guiar a governança ética para que o Brasil avance com a regulação e prática empresarial alinhadas aos padrões globais, promovendo uma IA que respeite os direitos humanos e seja transparente e responsável. Celso Azambuja reforça que incorporar as melhores práticas internacionais aos contextos brasileiros é decisivo para a sustentabilidade ética da tecnologia no país (AZAMBUJA, 2024).

2.4 ANÁLISE CRÍTICA DAS LEGISLAÇÕES E A APLICAÇÃO PRÁTICA NA PROTEÇÃO DE DADOS PELAS BIG TECHS

A implementação das legislações brasileiras voltadas à proteção de dados, como a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet e a Lei Carolina Dieckmann, estabelecem um marco regulatório importante e inovador para assegurar direitos fundamentais

dos titulares de dados no contexto digital. No entanto, a aplicação destas normas pelas bus techs e startups revela algumas limitações e desafios significativos.

Em primeiro plano, a LGPD pioneira ao instituir princípios como finalidade, necessidade, transparência e segurança no tratamento de dados pessoais, representa uma evolução do ordenamento jurídico brasileiro ao aproximar-se dos padrões internacionais, como o GDPR europeu (Brasil, 2018). Contudo, sua efetividade depende da capacidade das organizações de garantir a adequação e conformidade contínua. Observa-se que muitas big techs, devido ao volume massivo de dados com que operam, enfrentam dificuldades na implementação completa de mecanismos técnicos e administrativos exigidos pela LGPD, principalmente em relação à governança de dados sensíveis e consentimento informado (Peck, 2021).

O Marco da Internet, por sua vez, ao estabelecer direitos dos usuários e responsabilização dos provedores, é fundamental para a proteção da privacidade no espaço virtual. Não obstante, sua aplicação em casos concretos muitas vezes esbarra na complexidade técnica da identificação do responsável por danos decorrentes dos da IA, dada a opacidade dos algoritmos e processos automatizados empregues pelas big techs (Gomes et al., 2020).

No âmbito penal, a Lei Carolina Dieckmann visa coibir invasões e crimes digitais, ponto crucial num ambiente de crescente vulnerabilidade cibernética. Porém, o ritmo acelerado das inovações tecnológicas põe à prova a capacidade do sistema penal de responder a novas modalidades de crimes envolvendo IA e tratamento indevido de dados (TEIXEIRA, 2024).

Outro aspecto importante é o equilíbrio entre o avanço tecnológico proporcionado pela IA e a necessidade de privacidade e proteção dos dados pessoais. Embora as big techs invistam em soluções de segurança, incidentalmente há riscos constantes de vazamentos e uso inadequado de informações (web). Assim, apesar das legislações existentes, falta um mecanismo mais robusto de auditoria independente e transparência que garanta a efetiva fiscalização e controle das práticas dessas empresas.

Isto sem mencionar os desafios éticos ligados à automatização das decisões que podem criar discriminação algorítmica e a falta de clareza sobre como as decisões são tomadas, questões ainda pouco regulamentadas, mas fundamentais para a consolidação da confiança dos usuários no sistema digital (Cath et al., 2018)

Em suma, ainda que as legislações brasileiras estabeleçam bases legais adequadas, sua implementação plena e fiscalização exigem maior integração entre poderes públicos, sociedade civil e setor privado. Recomenda-se investir na capacitação técnica, aprimorar políticas de

governança de dados e fomentar a adoção de tecnologias que aumentem a transparência e o controle social.

2.5 ESTUDO DE CASOS

Para ilustrar os desafios e a complexidade da proteção de dados pessoais em big techs que utilizam inteligência artificial, destacam-se alguns casos recentes e emblemáticos.

Um projeto de pesquisa divulgado em 2021⁵ revelou o maior vazamento de dados da história, que expôs 16 bilhões de senhas e credenciais de login vinculadas a grandes empresas como Apple, Google, Meta (Facebook, Instagram e WhatsApp), Telegram e GitHub, além de serviços governamentais³. A investigação identificou 30 conjuntos de dados inéditos, contendo registros em escala bilionária, organizados de forma a facilitar ataques automatizados e invasões em larga escala. Esse caso evidenciou a vulnerabilidade dos sistemas diante da exploração em massa por agentes maliciosos, destacando a importância de medidas robustas de segurança e governança de dados pelas big techs.

Outro exemplo seria o incidente que ocorreu com a plataforma chinesa de IA DeepSeek, que sofreu um vazamento de mais de 1 milhão de dados sensíveis, incluindo históricos de conversas chaves criptografadas. Esse episódio, reportado em 2025, revela os riscos crescentes da utilização de IA sem proteção adequada e a necessidade de adoção de estratégias eficazes de cibersegurança, capaz de antecipar e neutralizar ataque e falhas sistêmicas.⁴

O incidente envolveu o vazamento de mais de um milhão de dados sensíveis, incluindo históricos de conversas e chaves criptografadas, foi detalhadamente investigado por pesquisadores de cibersegurança. O vazamento ocorreu devido a uma base de dados ClickHouse exposta, acessível publicamente sem autenticação, permitindo controle total sobre as operações do banco de dados e acesso a informações confidenciais (Wiz Research, 2025). Após a divulgação da fragilidade pela Wiz Research, a DeepSeek com fito de conter o vazamento de dados, adotou medidas imediatas, ainda assim o episódio demonstrou graves riscos na segurança de dados em plataformas de IA.

³ OLHAR DIGITAL. Bilhões de senhas do Google, Apple e Meta teriam sido roubadas em vazamento gigantesco. Disponível em: <https://olhardigital.com.br/2025/06/20/seguranca/maior-vazamento-da-historia-bilhoes-de-senhas-do-google-apple-e-meta-teriam-sido-roubadas/>. Acesso em: 10 de out, 2025.

⁴ FORBES Brasil. Acusações, Vazamentos e Restrições: DeepSeek Entra na Mira dos Concorrentes. Disponível em: <https://forbes.com.br/forbes-tech/2025/01/acusacoes-vazamentos-e-restricoes-deepseek-entra-na-mira-dos-concorrentes/>. Acesso em: 3 out. 2025.

Ademais, há também riscos abrangendo ética e privacidade. A recente intervenção da Autoridade Nacional de Proteção de Dados (ANPD) relacionada à Meta Platforms Inc. exemplifica a tensão entre inovação tecnológica e direitos fundamentais. A ANPD suspendeu uma política da Meta que permitia o uso extensivo de dados pessoais para o treinamento de IA generativa, destacando a necessidade de observância estrita da legislação e da proteção aos direitos dos titulares. Essa decisão marca um precedente importante para a governança de IA no Brasil, indicando que a conformidade legal não pode ser negligenciada frente ao avanço tecnológico.

Há também exemplos positivos, como a adaptação de empresas à LGPD, como o YouTube Kids⁵, que implementou controles específicos para proteger dados de crianças, requerendo o consentimento de responsáveis e oferecendo mecanismos para gerenciar o acesso ao conteúdo, este caso demonstrar que, com planejamento e políticas claras, é possível conciliar inovação com proteção efetiva de dados pessoais.

O “ECA Digital” – versão atualizada e adaptada do Estatuto da Criança e do Adolescente para o meio online – nasceu a partir de um contexto de profunda preocupação social com a exposição precoce e inadequada de crianças e adolescentes nas redes digitais. Em 2025, uma série de denúncias públicas ganhou destaque, em especial o vídeo publicado pelo influenciador Felipe Bressanim Pereira, conhecido como Felca, que mostrou a chamada adultização de menores nas redes sociais. Felca denunciou diferentes casos em que crianças e adolescentes eram sexualizados e expostos a conteúdos impróprios, o que gerou ampla repercussão na mídia e mobilizou parlamentares e organizações civis.⁶

Diante disto, os debates sobre a necessidade de ampliar a proteção dos direitos das crianças no ambiente digital ganharam fôlego. O Estatuto original de 1990, embora avançado para época, não contemplava as transformações provocadas pela popularização da internet, redes sociais, plataformas de vídeo e a disseminação acelerada de conteúdos digitais. Assim, percebeu-se a necessidade de atualizar a legislação para enfrentar questões específicas de segurança, privacidade e direitos fundamentais.

Diante desse cenário, nasce o Projeto de Lei nº 2.628, de 2022, batizado como ECA Digital. O projeto propôs medidas inéditas de espaços digitais, como a implementação de

⁵ YOUTUBE. Como o YouTube mantém as crianças seguras on-line. Disponível em: https://www.youtube.com/intl/ALL_br/howyoutubeworks/our-commitments/fostering-child-safety/.

⁶ G1. Após pedido de Felca, Justiça autoriza quebra de sigilo de 233 perfis que o chamaram de pedófilo e abusador. Disponível em: <https://g1.globo.com/pr/norte-noroeste/noticia/2025/08/13/felca-justica-autoriza-quebra-de-sigilo-de-233-perfis.ghtml>.

mecanismos de verificação de idade confiáveis, criação de espaços seguros para menores, responsabilização das plataformas digitais no controle de conteúdos nocivos como a exploração sexual, bullying, jogos de aposta e suicídio, e a exigência de supervisão parental efetiva. A lógica da legislação passa a focar não apenas no conteúdo, mas na arquitetura dos produtos digitais, determinando que sistemas e algoritmos sejam desenvolvidos para proteger os direitos da criança desde o design, incorporando o conceito de “proteção pela concepção” (privacy/safety by design)⁷.

Desde de 2022 há um projeto sobre o tema PL 2628/2022 de autoria do Senador Alessandro Veira de Sergipe. A tramitação acelerada do projeto foi motivada pela urgência do tema e pela pressão social, culminando com a sanção da Lei nº 15.211, em 17 de setembro de 2025, pelo presidente da República. Esta legislação pioneira no Brasil estabelece regras claras para produtos e serviços digitais que sejam destinados ou possam ser acessados por crianças e adolescentes, promovendo maior segurança e controle por parte dos responsáveis, prevendo ainda sanções para violações, fortalecendo a governança digital voltada à infância.⁸

O ECA Digital marca um importante avanço no campo da proteção infantil, colocando o Brasil entre os países que adotam legislações progressistas e abrangentes para a realidade digital atual e futura. Tal lei reflete a compreensão de que a infância conectada exige uma guarda efetiva dos direitos dos menores, assegurando que a tecnologia seja uma aliada do seu desenvolvimento saudável e não uma fonte de riscos e violações.

Por último, destaca-se o caso do assistente de IA Microsoft Copilot, o qual apresentou fragilidades de segurança exploráveis por atacantes para exfiltrar dados e realizar ataques de phishing invisíveis, conforme demonstrado em conferências especializadas. Esse episódio demonstrou a necessidade constante de testes, atualizações e auditorias de segurança em sistemas baseados em IA para garantir a proteção dos dados processados.

Tais casos evidenciam a complexidade do desafio das big techs em implementar sistemas de IA que garantam a segurança, privacidade e respeito à legislação vigente, reforçando a necessidade de uma abordagem integrada e multidisciplinar para a governança de dados na era digital.

3 CONSIDERAÇÕES FINAIS

⁷ É uma abordagem proativa de proteção da privacidade que visa incorporar medidas de segurança e privacidade desde a concepção de um produto ou serviço, e não apenas como uma adição post

⁸ BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Dispõe sobre a proteção de crianças e adolescentes em ambientes digitais, institui o Estatuto Digital da Criança e do Adolescente, e dá outras providências. Diário Oficial da União, Brasília, 17 set. 2025

Este estudo permitiu compreender em profundidade a magnitude e o impacto da inteligência artificial (IA) nas operações das big techs e startups, destacando seu papel transformador na oferta de serviços e na otimização de processos. A análise evidenciou que, apesar dos ganhos substanciais e da eficiência, a incorporação dessa tecnologia traz consigo desafios complexos, especialmente no campo da proteção de dados pessoais. É evidente que o ordenamento jurídico brasileiro precisa não apenas acompanhar, mas antecipar-se a essas transformações a fim de assegurar os direitos fundamentais à privacidade e à segurança da informação, visto que estes são pilares essenciais numa sociedade democrática e digitalizada.

Nesse contexto de avanços tecnológicos e crescente digitalização, o Brasil deu um passo importante com a aprovação da Lei nº 15.211, denominada de Estatuto Digital da Criança e do Adolescente (ECA Digital), sancionada em setembro de 2025. A aprovação do ECA Digital foi motivada por preocupações sociais sobre a exposição indevida de crianças e adolescentes em ambientes digitais, intensificada por denúncias públicas e escândalos de “adultização” precoce de menores nas redes sociais e plataformas digitais. Diante das denúncias tornou-se evidente a necessidade da atualização do Estatuto da Criança e do Adolescente, originalmente concebido em 1990, com fito de garantir também a ampla proteção no meio virtual.

O arcabouço normativo brasileiro, com a LGPD, o Marco Civil da Internet e a Lei Carolina Dieckmann, já dispunha de importantes ferramentas legais para a proteção dos usuários. Todavia, a aprovação do ECA Digital representou um avanço ao estabelecer regras específicas para produtos e serviços digitais acessados por crianças e adolescentes, como a verificação de idade, supervisão parental, proibição de conteúdo impróprio e publicidade dirigida, além de responsabilizar as plataformas por práticas nocivas. Deste modo, a legislação brasileira reconhece e atua sobre os riscos específicos do meio digital, especialmente protegendo o público infantojuvenil.

Entretanto, a aplicação efetiva dessas normas ainda enfrenta obstáculos técnicos administrativos e éticos que transcendem o mero cumprimento formal. As lacunas existentes na governança e fiscalização, somadas à complexidade da IA e dos ambientes digitais, reforçam a necessidade de uma atuação integrada do Estado, setor privado e comunidade acadêmica para prevenir e minimizar os riscos decorrentes do uso inadequado dessas inovações, garantindo um ambiente digital mais seguro e justo para todos.

Ademais, as questões éticas relacionadas à tomada de decisões automatizadas nos sistemas de IA chamam a atenção para demandas de transparência, equidade e responsabilidade

no desenvolvimento tecnológico. A busca por políticas empresariais mais robustas e investimentos contínuos em inovação regulatória e segurança da informação são indispensáveis para equilibrar o ritmo acelerado da transformação digital com a salvaguarda dos direitos fundamentais dos titulares de dados, assim trazendo harmonia entre tecnologia e ética devendo este ser o objetivo maior para assegurar que progresso tecnológico traga benefícios sociais reais.

Portanto, a governança da IA e a proteção de dados não podem ser encaradas como problemas isolados ou exclusivamente técnicos e legais, mas como desafios multidimensionais que envolvem aspectos jurídicos, sociais e culturais. Construir um ambiente digital, justo e confiável se exige um esforço coletivo, pautado no diálogo entre políticas públicas, práticas empresariais responsáveis e a participação ativa da sociedade civil, deste modo será possível assegurar que a inteligência artificial, de fato, seja uma ferramenta de evolução alinhada aos valores humanos essenciais.

Por fim, esta pesquisa pode servir como base para futuros aprofundamentos, ressaltando a importância do debate acadêmico e institucional acerca dos novos paradigmas impostos pela IA. Para posteriores pesquisas é possível a exploração de temas complementares, como a governança internacional da IA, implicações sociais da automação e evolução dos mecanismos de fiscalização e responsabilização, sempre com foco na promoção dos direitos e garantias fundamentais.

REFERÊNCIAS

- A Inteligência Artificial e a Privacidade de Dados: Entenda a relação. Disponível em: <https://peduti.com.br/.artigo/ia-e-privacidade-de-dados/>. Acesso em: 2 nov. 2025.
- AZAMBUJA, Celso. Princípios internacionais para governança ética da inteligência artificial: uma visão brasileira. *Revista Brasileira de Ética e Tecnologia*, v. 4, n. 1, 2024.
- Brasil. (2012). Lei Carolina Dickmann. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm
- Brasil. (2014). Marco Civil da Internet - Lei nº 12.965, de 23 de abril de 2014. Diário Oficial da União.
- Brasil. (2018). Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União.
- CNBSP. IA e proteção de dados: desafios regulatórios e o caso da Meta Platforms. Disponível em: <https://cnbsp.org.br/2024/07/05/artigo-ia-e-protECAo-de-dados-desafios-regulatórios-e-o-caso-da-meta-platforms-por-jorge-alexandre-fagundes/>. Acesso em: 2 nov. 2025.
- Direito Constitucional e Tecnologia: Novos Desafios. Editora Revista dos Tribunais, 2022.
- FEFERBAUM, Marina. A importância da capacitação e ética na governança de inteligência artificial. In: CONGRESSO NACIONAL DE INFORMÁTICA E DIREITO, 22., 2023, Rio de Janeiro. Anais... Rio de Janeiro: Editora do Congresso, 2023.
- FRAZÃO, Ana Luiza. Estratégias integradas de proteção de dados e segurança na inteligência artificial. In: CONGRESSO BRASILEIRO DE DIREITO DIGITAL, 15., 2023, São Paulo. Anais. São Paulo: Editora Jurídica Nacional, 2023.
- GALICIA EDUCAÇÃO. Controle das Big Techs sobre IA: riscos e regulamentação. Disponível em: <https://www.galiciaeducacao.com.br/blog/controle-das-big-techs-sobre-ia-riscos-e-regulamentacao/>. Acesso em: 10 out. 2025.
- Gil, A. C. Métodos e Técnicas de Pesquisa Social. São Paulo: Atlas, 2008.
- Gomes, A., Silva, R., & Souza, J.** Direito digital e proteção de dados pessoais no Brasil. *Revista Brasileira de Direito Digital*, 2020.
- GRANT THORNTON. IA e Privacidade: desafios regulatórios para proteção de dados. Disponível em: <https://grantthornton.com.br/insights/artigos-e-publicacoes/ia-e-privacidade-desafios-regulatorios-para-protECAo-de-dados/>. Acesso em: 30 abr. 2025.
- GRANT THORNTON. IA e Privacidade: desafios regulatórios para proteção de dados. Disponível em: <https://grantthornton.com.br/insights/artigos-e-publicacoes/ia-e-privacidade-desafios-regulatorios-para-protECAo-de-dados/>. Acesso em: 21 jun. 2025.

IA na segurança e privacidade de dados: impactos, riscos e soluções. Disponível em: <https://zendesk.com.br/blog/ia-na-seguranca-e-privacidade-de-dados/>. Acesso em: 2 nov. 2025.

IBM. O que é transparência de IA? | IBM. Disponível em: <https://www.ibm.com/br-pt/think/topics/ai-transparency>. Acesso em: 03 mai. 2025.

ITFORUM. Inteligência Artificial sem proteção adequada abre lacuna de riscos e incidentes de segurança. Disponível em: <https://itforum.com.br/noticias/inteligencia-artificial-sem-protacao-lacuna-riscos/>. Acesso em: 1 nov. 2025.

KAUFMAN, Dora. Regulamentação ética da inteligência artificial: desafios e perspectivas brasileiras. *Revista Direito e Tecnologia*, v. 9, n. 1, 2023.

KPMG. Privacidade em um Novo Mundo de IA. Disponível em: <https://kpmg.com/br/pt/home/insights/2023/12/desafio-privacidade-mundo-crescente-uso-ia.html>. Acesso em: 10 ago. 2025.

Lei Carolina Dieckmann - Lei nº 12.737, de 30 de novembro de 2012. Diário Oficial da União.

MINDETEK. Quais são os desafios éticos da Inteligência Artificial? Disponível em: <https://www.mindtek.com.br/2025/09/quais-sao-os-desafios-eticos-da-inteligencia-artificial/>. Acesso em: 30 set. 2025.

PINHEIRO, Patrícia P. Direito Digital - 7ª Edição 2021. 7. ed. Rio de Janeiro: Saraiva Jur, 2021.

PEDUTI. A Inteligência Artificial e a Privacidade de Dados: Entenda a relação. Disponível em: <https://peduti.com.br/.artigo/ia-e-privacidade-de-dados/>. Acesso em: 2 nov. 2025.

PORTAL PUC-RS. Proteção de dados pessoais: avanços, desafios e o impacto da inteligência artificial. Disponível em: <https://portal.pucrs.br/noticias/inovacao/protacao-de-dados-pessoais-avancos-desafios-e-o-impacto-da-inteligencia-artificial/>. Acesso em: 2 nov. 2025.

Proteção de dados pessoais: avanços, desafios e o impacto da inteligência artificial. Disponível em: <https://portal.pucrs.br/noticias/inovacao/protacao-de-dados-pessoais-avancos-desafios-e-o-impacto-da-inteligencia-artificial/>. Acesso em: 29 out. 2025.

REVISTA TÓPICOS. Gestão e tecnologia: desafios éticos e jurídicos na implementação da inteligência artificial nas corporações. Disponível em: <https://revistatopicos.com.br/artigos/gestao-e-tecnologia-desafios-eticos-e-juridicos-na-implimentacao-da-inteligencia-artificial-nas-corporacoes>. Acesso em: 5 mai. 2025.

SAFETEC. Segurança em inteligência artificial: como garantir?. Disponível em: <https://safetec.com.br/inteligencia-artificial/seguranca-em-inteligencia-artificial/>. Acesso em: 12 set. 2025.

SANTOS, Edson. Responsabilidade civil nas decisões automatizadas: um estudo sobre lacunas normativas brasileiras. *Revista Jurídica Contemporânea*, v. 17, n. 3, 2024.

SERPRO. Ética na IA. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2023/etica-na-ia>. Acesso em: 2 jun. 2025.

TEIXEIRA, Tarcisio. Direito Digital e Processo Eletrônico - 8ª Edição 2024. 8. ed. Rio de Janeiro: Saraiva Jur, 2024.

UNESCO. Ética da Inteligência Artificial (IA) no Brasil. Disponível em: <https://www.unesco.org/pt/fieldoffice/brasil/expertise/artificial-intelligence-brazil>.

Acesso em: 2 nov. 2025.

ZAVAGLIA, Alexandre. Transparência e explicabilidade em sistemas de inteligência artificial: barreiras e soluções. *Revista de Direito, Tecnologia e Sociedade*, v. 8, n. 2, 2023.

ZENDESK. IA na segurança e privacidade de dados: impactos, riscos e soluções. Disponível em: <https://zendesk.com.br/blog/ia-na-seguranca-e-privacidade-de-dados/>. Acesso em: 2 nov. 2025.