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

PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E NEGÓCIOS INOVADORES II

P961
Privacidade, proteção de dados pessoais e negócios inovadores II [Recurso eletrônico on-line] organização VI Congresso Internacional de Direito e Inteligência Artificial (VI CIDIA): Skema Business School – Belo Horizonte;

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

Inclui bibliografia
ISBN: 978-65-5274-361-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Perspectivas globais para a regulação da inteligência artificial.
1. GDPR. 2. Segurança da informação. 3. Compliance. I. VI Congresso Internacional de Direito e Inteligência Artificial (1:2025 : Belo Horizonte, MG).

CDU: 34

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

PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS E NEGÓCIOS INOVADORES II

Apresentação

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Ms. Dorival Guimarães Pereira Júnior

Coordenador do Curso de Direito – SKEMA Law School

Prof. Dr. José Luiz de Moura Faleiros Júnior

Coordenador de Pesquisa – SKEMA Law School

REGULAÇÃO DE NOVAS TECNOLOGIAS EM M&AS: POSSÍVEIS IMPACTOS TRAZIDOS PELA REGULAÇÃO DA PROTEÇÃO DE DADOS E DA INTELIGÊNCIA ARTIFICIAL PARA OPERAÇÕES NO BRASIL

REGULATING EMERGING TECHNOLOGIES IN M&A: POTENTIAL IMPACTS OF DATA PROTECTION AND ARTIFICIAL INTELLIGENCE FRAMEWORKS ON BUSINESS TRANSACTIONS IN BRAZIL

Jamile Sabbad Carecho Cavalcante [1]
Mateus Reis dos Santos Alves [2]
Maria Eugenia de Araújo Vianna [3]

Resumo

Este artigo examina, de forma integrada, o estado atual da regulação da inteligência artificial (IA) e da proteção de dados no Brasil e discute como esses regimes jurídicos impactam operações de fusões e aquisições (mergers and acquisitions - M&As) envolvendo empresas do setor de tecnologia. Inicialmente, contextualizase a rápida digitalização da economia brasileira e o papel catalisador da IA na reconfiguração de processos corporativos. Em seguida, analisam-se os principais diplomas normativos relacionados à proteção de dados nacionais — a Lei Geral de Proteção de Dados (LGPD) e as resoluções da Autoridade Nacional de Proteção de Dados (ANPD) — à luz debenchmarks internacionais. Por fim, explora impactos diretos da IA e das regras de proteção de dados pessoais acima mencionadas em operações de M&A no mercado brasileiro. O estudo adota metodologia exploratóriadescritiva, com pesquisa documental e análise comparada de casos. Concluise que lacunas de enforcement e eventuais sobreposições regulatórias elevam os custos de conformidade, mas iniciativas que aumentam a segurança jurídica podem fomentar inovação e dinamizar o mercado de M&A no Brasil.

Palavras-chave: Inteligência artificial, Proteção de dados pessoais, Fusões e aquisições, Due diligence

Abstract/Resumen/Résumé

mergers and acquisitions (M&A) involving companies from the technology sector. Initially, the paper contextualises the fast digitalisation of the Brazilian economy and AI's catalytic role in reshaping corporate processes. In sequence, it analyses the main rules related to data privacy in Brazil — the General Data Protection Law (LGPD) and the National Data Protection Authority's (ANPD) resolutions — in light of international benchmarks. Finally, it explores the direct impacts of AI and data protection rules mentioned above in M&A transactions carried out in the Brazilian market. This paper uses an exploratorydescriptive methodology based on documentary research and comparative case analysis. It concludes that enforcement gaps and potential regulatory overlaps increase compliance costs, although instruments to guarantee legal security can enhance innovation and develop the M&A market in Brazil.

Keywords/Palabras-claves/Mots-clés: Artificial intelligence, Personal data protection, Mergers and acquisitions, Due diligence

Introdução

A economia brasileira atravessa, desde meados da década passada, um processo de digitalização acelerada, impulsionado pelo amadurecimento de *start-ups* locais, pelo barateamento da computação em nuvem e por políticas públicas de fomento à inovação (OCDE, 2023).

Nesse cenário, a Inteligência Artificial (IA) deixou de ser mera prova de conceito para ocupar posição central nas estratégias corporativas, transformando empresas em fornecedoras de *software*, gestoras de grandes volumes de dados e desenvolvedoras de modelos preditivos. Consequentemente, ativos intangíveis, sobretudo *datasets*, algoritmos e *know-how*, passaram a compor parcela determinante do valuation de companhias de base tecnológica, atraindo investidores e compradores nacionais e estrangeiros (KPMG, 2024).

Essa mutação repercute na mecânica de fusões e aquisições, ou em inglês, *mergers & acquisitions*, (*M&A):* cada transação precisa aferir, com rigor, o valor econômico de sistemas algorítmicos e o grau de exposição a passivos regulatórios decorrentes do tratamento de dados pessoais.

A criação da Autoridade Nacional de Proteção de Dados (ANPD) e a vigência da Lei Geral de Proteção de Dados (LGPD), desde 2020, consolidaram um marco jurídico robusto que impõe obrigações de segurança, bases legais estritas e sanções financeiras expressivas (Brasil, 2018). Paralelamente, o Projeto de Lei n.º 2.338/2023, tramitando na Câmara dos Deputados desde março de 2025, adota abordagem baseada em risco, exigindo avaliação de impacto algorítmico, governança de dados e auditoria contínua (Brasil, 2023). No plano internacional, o *Artificial Intelligence Act (AI ACT)* europeu já influencia documentos de *due diligence* no Brasil, pois compradores globais demandam aderência aos seus parâmetros (União Europeia, 2024).

Embora esse arcabouço encampe a noção de "centralidade da pessoa humana", persiste o desafio de calibrar a densidade regulatória sem inibir a inovação. A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) recomenda regulação proporcional e baseada em risco, advertindo que sobreposições normativas excessivas podem desestimular investimentos e retardar benefícios sociais. Como destaca Cavalcante (2024, p. 172), "a regulação da tecnologia não impede o avanço da inteligência artificial, mas garante

que o progresso acontecerá de maneira séria, segura, ética e responsável pautado nos direitos fundamentais."

Estudos recentes demonstram que o peso do *compliance* tem consumido parcela crescente do orçamento de Tecnologia da Informação (TI) das empresas de alto crescimento no Brasil. Levantamento da *LexisNexis Risk Solutions* em parceria com a *Forrester Consulting* revela que 97 % das instituições financeiras latino-americanas registraram aumento substancial nos gastos com conformidade em 2023, impulsionados sobretudo por investimentos em tecnologias de dados e em soluções de IA voltadas à prevenção de riscos regulatórios.

O cenário doméstico é corroborado pela 2ª Pesquisa Nacional sobre Tendências em *Compliance*, segundo a qual 62 % dos profissionais brasileiros de compliance consideram o orçamento já inferior às suas necessidades, enquanto 56 % não projetam qualquer ampliação de recursos para 2025, tendência que se agrava durante processos de due diligence e operações de *M&A,* quando as exigências regulatórias se tornam mais rigorosas (*LexisNexis Risk Solutions; Forrester Consulting*, 2024) (Aliant; Protiviti, 2025). Esses números confirmam que, mesmo sem percentuais absolutos uniformes, as *scale-ups* destinam fração cada vez mais significativa de seus investimentos tecnológicos à adequação jurídica, reforçando a importância de programas de governança de dados desde a fase inicial de crescimento.

Em complemento, estudos recentes indicam que a pressão orçamentária para *compliance* se intensifica nas fases de *due-diligence*: a KPMG constatou que 65 % dos investidores já esbarraram em achados *ESG* (*Environmental, Social and Governance,* ou, em português Ambiental, Social e Governança) capazes de travar ou renegociar o negócio (KPMG, 2024), enquanto a BCG calcula que uma análise *ESG* minuciosa protege até 10 % do valor da operação *(Boston Consulting Group,* 2024). No plano cibernético, reportagem da Reuters mostra que falhas de segurança detectadas na auditoria podem inviabilizar acordos ou resultar em multas relevantes, ampliando o custo regulatório dos compradores (Sagar, 2025).

Com vistas a equilibrar proteção de direitos e estímulo ao progresso tecnológico, o Projeto de Lei n.º 2.338/2023 estabelece, nos arts. 38 a 41, a criação de um *sandbox* regulatório de inteligência artificial, permitindo que soluções inovadoras sejam testadas sob supervisão mitigada e por prazo determinado (Brasil, 2023). A opção pelo *sandbox* não é

inédita no ordenamento brasileiro: a experiência do Banco Central do Brasil, inaugurada pela Resolução BCB n.º 29/2020 (Banco Central do Brasil, 2020), e a do mercado de capitais, iniciada pela Instrução CVM n.º 626/2020 (Comissão de Valores Mobiliários, 2020), demonstram a utilidade do mecanismo ao viabilizar testes controlados de novos modelos de negócio, promover interação direta com o regulador e antecipar ajustes normativos antes da oferta plena ao mercado

Todavia, o fator humano continua a ser a peça de maior risco em qualquer transação. O episódio Arezzo & Co ↔ Grupo Soma ilustra bem esse ponto: anunciada em 2023, a combinação que formaria a Azzas 2154 sofreu abalos públicos em março de 2025, quando divergências de estilo de gestão e disputas de protagonismo fizeram o mercado precificar uma possível cisão e derrubaram as ações em mais de 10 % (Central do Varejo, 2025; Investalk, 2025). A literatura de governança reforça que essa tensão não é exceção: levantamento global da Deloitte mostra que cerca de 30 % das operações de *M&A* fracassam justamente porque algoritmos de valuation ignoram variáveis subjetivas — compatibilidade cultural, retenção de talentos e liderança — que só afloram na fase de integração (Deloitte, 2025).

Conforme mencionado e demonstrado anteriormente, muito embora existam estudos sobre *compliance* de dados e sobre os efeitos regulatórios em operações de *M&A*, existe uma ausência de trabalhos que construam essas duas frentes em relação ao novo arcabouço brasileiro de inteligência artificial.

Portanto, a lacuna está em compreender, de forma integrada, como a sobreposição entre a LGPD, o Projeto de Lei nº 2.338/2023 e as cláusulas contratuais "importadas" do *AI Act* europeu interferem, de modo benéfico ou não, no ciclo de *M&A* envolvendo empresas de base tecnológica. Em outras palavras, é preciso saber se esse mosaico regulatório cria um ambiente de segurança jurídica que estimula transações ou, ao contrário, introduz custos e incertezas que podem frear o apetite de investidores estratégicos e fundos de private equity

Por isso, o trabalho busca responder à seguinte pergunta: Quais ajustes regulatórios e práticas contratuais podem transformar o Brasil em *hub* regional de *M&A* em IA, sem sacrificar a proteção de dados e o protagonismo humano? Para isso, tem como objetivo a compreensão evidenciada na lacuna de pesquisa, apta a responder o presente problema.

Adotou-se metodologia exploratória-descritiva com análise dedutiva documental de diplomas legislativos a partir da análise do *AI Act* europeu e de estudo de casos emblemáticos de *M&A* no Brasil, elegendo como recorte empírico transações envolvendo ativos de IA e *big data*. Resta destacar ainda que, aspectos concorrenciais perante o Conselho Administrativo de Defesa Econômica (CADE) e questões tributárias escapam ao escopo deste estudo.

O trabalho será organizado em três partes, serão elas: i) panorama da regulação de IA; ii) normas de proteção de dados e desafios de compliance; iii) impactos combinados sobre *M&A*, culminando com recomendações e agenda de pesquisa futura.

1. A Atual Regulação de IA no Brasil

1.1. Iniciativas Regulatórias e Processo Legislativo

A regulação voltada para a Inteligência Artificial (IA) dentro do território Brasileiro evoluiu de forma considerável desde o ano de 2018, principalmente por meio da Lei Geral de Proteção de Dados, mais conhecida como LGPD ou Lei nº 13.709/2018 (Brasil, 2018).

A LGPD trouxe dispositivos relevantes para a regulação indireta da IA, especialmente o artigo 20, que prevê o direito do titular à revisão de decisões automatizadas que impactem seus interesses pessoais, profissionais ou financeiros. Tal direito é reforçado pelos princípios da transparência e da não discriminação, previstos respectivamente no art. 6º, incisos VI e VIII, que exigem das empresas a oferta de informações claras sobre os processos de tratamento, inclusive quanto à lógica utilizada nos algoritmos.

A transparência figura como um dos princípios centrais da Lei Geral de Proteção de Dados Pessoais (LGPD), impondo às organizações a obrigação de fornecer informações claras, acessíveis e compreensíveis sobre todas as etapas do tratamento de dados pessoais.

Essa transparência deve ir além da simples apresentação dos dados tratados, abrangendo também o funcionamento dos sistemas automatizados e os modelos de negócio que os sustentam. Isso visa possibilitar que o titular compreenda, de maneira concreta, a legalidade, a finalidade e a legitimidade das operações de tratamento, promovendo a confiança no uso de tecnologias baseadas em algoritmos (Doneda, 2025). Dessa forma, a legislação não apenas impõe a obrigação de informar, mas exige que o responsável pela

decisão automatizada seja capaz de justificar, de forma compreensível, a lógica adotada na decisão, o que pressupõe a participação efetiva de pessoa natural para contextualizar e validar o resultado apresentado pelo sistema (Goulart, 2022).

Por outro lado, o princípio da não discriminação funciona como um mecanismo crucial contra vieses algorítmicos, especialmente quando são utilizados dados sensíveis, potencialmente ampliando vulnerabilidades sociais e econômicas (Mulholland; Frajhof, 2019).

Muito embora essas disposições tivessem inaugurado um regime mínimo para lidar com riscos algorítmicos, a LGPD não foi originalmente desenhada para regular de forma abrangente as particularidades técnicas e éticas dos sistemas de inteligência artificial, o que evidencia a necessidade de normas complementares e instrumentos específicos de governança algorítmica, aptos a responder a questões como discriminação, explicabilidade e *accountability* em modelos cada vez mais sofisticados, conforme ressaltado por Bioni, *et al*. (2023).

No contexto da evolução regulatória da IA no Brasil, o Projeto de Lei nº 21/2020 representou uma primeira tentativa de instituir diretrizes nacionais, mas se mostrou, desde o início, excessivamente principiológico e carente de densidade normativa. O texto, composto por apenas 22 artigos, foi criticado por especialistas do setor e por organizações da sociedade civil por não apresentar critérios objetivos de avaliação de risco, tampouco mecanismos claros de fiscalização e accountability, além de não integrar tecnicamente as salvaguardas previstas na Lei Geral de Proteção de Dados (LGPD) (*Data Privacy* Brasil, 2021).

A partir de 2022, a agenda nacional passou a ser substancialmente aprimorada com a instalação da Comissão de Juristas sobre Inteligência Artificial (CJSUBIA), instituída pelo Senado Federal. O objetivo deste colegiado foi justamente suprir as lacunas identificadas no PL 21/2020, alinhando o debate regulatório brasileiro a parâmetros internacionais, como os princípios da OCDE para IA e as discussões que culminaram no *AI Act* europeu (*Data Privacy* Brasil, 2023).

Desse processo nasceu o Projeto de Lei nº 2.338/2023, como aponta Cavalcante (2024), “o PL nº 2.338/2023 representa uma tentativa concreta de estruturar um marco legal robusto para sistemas de IA, adotando critérios de risco e prevendo a obrigatoriedade de mecanismos como a avaliação de impacto algorítmico, a explicabilidade de decisões

automatizadas e o sandbox regulatório". Também propõe um modelo de co-regulação no qual a Autoridade Nacional de Proteção de Dados (ANPD) assume o papel de coordenação transversal, articulando-se com agências setoriais que detêm expertise regulatória em áreas como saúde, finanças e Justiça (*Data Privacy* Brasil, 2024).

Importa ainda registrar que a discussão legislativa ganhou densidade a partir da instituição da Comissão Temporária Interna sobre IA (CTIA), responsável por coordenar audiências públicas e conduzir revisões técnicas do texto do PL nº 2.338/2023. Os relatórios e pareceres produzidos por essa comissão buscaram responder a novos desafios, como o avanço da IA generativa e a crescente demanda social por transparência, explicação e mecanismos de contestação de decisões automatizadas, especialmente em períodos eleitorais e em setores críticos como o Judiciário (*Data Privacy* Brasil, 2024; Rodrigues; Mendonça; Nóvoa, 2025).

Posteriormente, em 2023, foi instituída pelo Senado a Comissão Temporária Interna sobre Inteligência Artificial (CTIA), que realizou 19 audiências públicas e diversas revisões do projeto, buscando especialmente endereçar novos desafios impostos pela disseminação da IA generativa, exemplificada pelo lançamento do GPT-4, e pelas demandas decorrentes das eleições de 2024 quanto ao controle de *deepfakes* e manipulações políticas (Senado Federal, 2024; Agência Senado, 2023; CeMEAI/USP, 2023). Após detalhada revisão, o Senado aprovou a versão final do texto em dezembro de 2024, encaminhando-o para análise da Câmara dos Deputados em março de 2025 (Senado Federal, 2025).

Apesar dos avanços institucionais e do amadurecimento do debate regulatório sobre IA no Brasil, a aprovação definitiva de um marco legal robusto enfrenta entraves consideráveis, diante de um tensionamento entre centralização e descentralização da regulação, prejudicando a tramitação célere do projeto.

O principal desafio reside no conflito de competências regulatórias: agências setoriais relevantes, como o Banco Central do Brasil (BACEN) e a Agência Nacional de Saúde Suplementar (ANS), pleiteiam maior autonomia para regulamentar aplicações de IA dentro de seus respectivos setores, em contrapartida ao papel de coordenação transversal almejado pela Autoridade Nacional de Proteção de Dados (ANPD) (*Data Privacy* Brasil, 2024).

Outro obstáculo relevante decorre da pressão de atores econômicos, especialmente startups, empresas de tecnologia e entidades representativas do setor digital, que manifestam

preocupação com o possível impacto financeiro e operacional decorrente da adoção de exigências como a Avaliação de Impacto Algorítmico (AIA) e o registro detalhado de logs de decisão (*Data Privacy* Brasil, 2023).

Por fim, há uma dimensão estratégica na postergação da aprovação do marco regulatório nacional: o Parlamento e diversos atores institucionais têm aguardado a consolidação de parâmetros internacionais, em especial com a publicação do *Artificial Intelligence Act* da União Europeia (União Europeia, 2024) e a *Executive Order* 14110 dos Estados Unidos (*United States*, 2023), com a ideia principal de evitar que o Brasil aprove um regime incompatível com padrões globais, prevenindo assimetrias que possam afastar investimentos estrangeiros ou criar dificuldades para empresas brasileiras que atuam em múltiplas jurisdições (*Data Privacy* Brasil, 2024).

Dessa forma, a trajetória regulatória brasileira na área de IA evoluiu substancialmente, ainda que persistam desafios para aprovação e implementação plena. Contudo, ainda persiste a definição de um marco normativo abrangente e equilibrado, que se mostra essencial não apenas para assegurar inovação tecnológica, mas também para proteger direitos fundamentais e garantir a confiança necessária dos diversos agentes econômicos envolvidos.

1.2. Marcos Normativos em Vigor

Entre os principais diplomas gerais destacam-se a Lei nº 12.965/2014, conhecida como Marco Civil da Internet (MCI), que estabelece princípios fundamentais como neutralidade de rede, privacidade e liberdade de expressão. O MCI prevê obrigações de guarda de registros e segurança mínima, que são aplicáveis indiretamente aos sistemas de IA utilizados em plataformas digitais e serviços online (Brasil, 2014). Complementando essa norma, o Decreto nº 8.771/2016 regulamenta aspectos específicos, impondo requisitos adicionais de segurança e detalhando práticas de gestão de logs e cooperação entre provedores para proteção contra incidentes cibernéticos (Brasil, 2016).

A Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709/2018), como já abordado rapidamente no tópico anterior, aprofunda essas obrigações, exigindo, além da segurança e privacidade dos dados, transparência nos processos automatizados, proteção contra discriminação e a realização obrigatória do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) em casos de alto risco (Brasil, 2018).

Especificamente sobre IA, o Decreto nº 10.332/2020 estabeleceu a Estratégia Brasileira de Inteligência Artificial (EBIA), representando o primeiro esforço governamental abrangente para orientar políticas públicas voltadas à tecnologia, promovendo diretrizes éticas e incentivos econômicos, além de introduzir a ideia do *sandbox* regulatório para testes supervisionados de novos sistemas (Brasil, 2020).

O Conselho Nacional de Justiça (CNJ), através das Resoluções nº 332/2020 e nº 615/2025, disciplinou o uso da IA no Poder Judiciário. As normas das resoluções exigem laudos periódicos de acurácia, transparência ativa sobre as funcionalidades e limitações dos algoritmos, e a supervisão humana constante nas decisões judiciais automatizadas, com o intuito de justamente evitar vieses injustos e, assim, preservar também a legitimidade das decisões judiciais (CNJ, 2025).

1.3. Órgãos Reguladores e suas Competências

Dentre os órgãos a serem citados neste tópico, a Autoridade Nacional de Proteção de Dados (ANPD), criada pela Medida Provisória nº 869/2018, convertida na Lei nº 13.853/2019, e posteriormente transformada em autarquia de natureza especial pela Lei nº 14.460/2022, é responsável por interpretar e fiscalizar a aplicação da Lei Geral de Proteção de Dados (LGPD), além de estabelecer normas e diretrizes sobre tratamento de dados pessoais (Brasil, 2022).

A atuação da Autoridade Nacional de Proteção de Dados (ANPD) ganhou relevância especial com a publicação da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, que regulamenta critérios e procedimentos para o tratamento de dados pessoais de alto risco, incluindo de forma expressa os dados sensíveis. Além disso, a resolução também definiu obrigações diferenciadas para agentes de tratamento de pequeno porte, com o objetivo de garantir equilíbrio entre proteção de dados e estímulo à inovação no ambiente digital brasileiro (ANPD, 2022).

Além disso, a Nota Técnica nº 19/2023/FIS/CGF/ANPD estabeleceu como temas prioritários para o biênio 2024/2025 a fiscalização de atividades envolvendo inteligência artificial e a prevenção de práticas discriminatórias (ANPD, 2023).

Há de ser destacada também as Resoluções CD/ANPD nº 4/2023 e nº 15/2024, que estabelecem diretrizes para a dosimetria das sanções e gestão de incidentes de segurança

envolvendo dados pessoais. Essas resoluções fixam penalidades expressivas, chegando a 2% do faturamento anual das empresas e impõem o prazo máximo de 48 horas para comunicação formal de incidentes, fortalecendo a *accountability* das empresas no tratamento responsável de dados pessoais em soluções tecnológicas avançadas (ANPD, 2024). Além da Autoridade Nacional de Proteção de Dados (ANPD), diversos outros órgãos reguladores exercem influência direta sobre o uso de IA e da tecnologia em seus respectivos setores.

O Banco Central do Brasil (BACEN), por exemplo, atuou inicialmente por meio das Resoluções nº 4.557/2017 e nº 255/2022, estabelecendo requisitos de transparência e governança rigorosa para o uso de IA em decisões financeiras, notadamente em operações de crédito e *open finance*. Em 2023, no entanto, tais normas foram atualizadas e integradas pela Resolução BCB nº 390/2023, que revogou a Resolução BCB nº 255/2022 e consolidou as exigências de políticas de segurança cibernética e governança de modelos algorítmicos em instituições financeiras (Banco Central do Brasil, 2023).

A Agência Nacional de Saúde Suplementar (ANS), por sua vez, através da Resolução nº 727/2022, regulamenta o uso de tecnologias preditivas na saúde suplementar, impondo requisitos rigorosos de validação clínica e obrigando as operadoras a realizar avaliações periódicas de impacto e manter canais efetivos de contestação para usuários afetados por decisões automatizadas (ANS, 2022).

No âmbito do Poder Judiciário, a regulação setorial da inteligência artificial tem sido exercida de maneira ativa pelo Conselho Nacional de Justiça (CNJ), cuja competência normativa decorre do artigo 103-B, §4º, inciso I da Constituição Federal de 1988. Como observa Cavalcante (2024, p. 92):

> O CNJ tem múltiplas funções na administração judiciária no Brasil, mas três se destacam: a) como órgão regulador; b) definidor, executor e articulador de políticas relacionadas ao sistema brasileiro de justiça multiportas; e c) laboratório, observatório e divulgador de boas práticas judiciais brasileiras (Cavalcante, 2024, p. 92)

A autora destaca ainda que o Conselho tem exercido papel fundamental no desenvolvimento e na regulação de sistemas inteligentes, por meio de atos normativos como as Resoluções CNJ nº 332/2020 e sua atualização por meio da Resolução nº 615/2025, e

outras medidas inseridas no escopo do Programa Justiça 4.0, evidenciando seu protagonismo na normatização da tecnologia aplicada à jurisdição.

Por fim, a Comissão de Valores Mobiliários (CVM) instituiu, por meio da Instrução nº 626/2020, o *sandbox* regulatório, mecanismo que permitiu que fintechs e *robo-advisors* testassem inovações tecnológicas em ambiente supervisionado antes da entrada definitiva no mercado formal. Esse regime experimental desempenhou papel relevante no fomento à inovação financeira, oferecendo maior segurança jurídica e reduzindo riscos regulatórios para startups e investidores. Posteriormente, a Instrução nº 626/2020 foi revogada pela Resolução CVM nº 29, que atualizou as regras e manteve o compromisso da autarquia com o incentivo à inovação e à modernização do sistema financeiro brasileiro (CVM, 2020; CVM, 2021).

2. A Regulação da Proteção de Dados Pessoais no Brasil

2.1. A Lei Geral de Proteção de Dados – LGPD

A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709/2018, trouxe uma mudança significativa ao ambiente de negócios no Brasil, impondo princípios e obrigações rigorosas quanto ao tratamento de dados pessoais. Essa lei baseia-se em diversos princípios fundamentais, entre eles finalidade, adequação, necessidade e transparência. Estes princípios determinam que os dados pessoais sejam coletados apenas para objetivos claros e legítimos, tratados adequadamente conforme esses objetivos, limitados ao mínimo necessário e informados de forma clara e acessível aos titulares dos dados (Brasil, 2018).

Os direitos conferidos aos titulares incluem o consentimento explícito, o direito de acesso, correção, eliminação e portabilidade dos dados, bem como o direito de oposição ao tratamento automatizado. Além disso, a LGPD estabelece que os controladores devem garantir segurança robusta aos dados tratados, prevenindo incidentes de segurança e vazamentos, alinhando-se com padrões internacionais de proteção de dados, como o GDPR europeu (União Europeia, 2016).

2.2. Demais Normas Aplicáveis

Além da LGPD, várias outras normas específicas complementam o quadro regulatório sobre proteção de dados no Brasil. O Marco Civil da Internet (Lei nº 12.965/2014) define diretrizes básicas de neutralidade, privacidade e proteção dos usuários na internet,

estabelecendo requisitos obrigatórios de segurança e manutenção de registros digitais, fundamentais para o compliance de empresas que operam com IA e big data (Brasil, 2014).

As Resoluções CD/ANPD nº 4/2023 e nº 15/2024 introduziram critérios rigorosos para a dosimetria das sanções administrativas e a comunicação de incidentes de segurança, estabelecendo a obrigatoriedade de notificação à ANPD em até 48 horas após o incidente. Normas setoriais específicas como as circulares do Banco Central (BACEN), especialmente a Resolução nº 255/2022, e a Resolução nº 727/2022 da Agência Nacional de Saúde Suplementar (ANS), detalham ainda mais as obrigações das instituições financeiras e operadoras de saúde na gestão de dados pessoais, especialmente no contexto do uso de inteligência artificial.

2.3. Obrigações das Empresas no Tratamento de Dados Pessoais

A LGPD impõe uma série de obrigações operacionais às empresas que realizam tratamento de dados pessoais, destacando-se seis pilares estratégicos:

2.3.1. Governança de dados

A governança de dados deixou de ser um diferencial para se tornar obrigação central nas organizações brasileiras, especialmente após o advento da LGPD. O artigo 50 impõe que empresas, sejam controladoras ou operadoras, implementem programas de governança capazes de demonstrar não só a adequação à lei, mas também a eficácia das medidas adotadas para proteger dados pessoais.

Isso significa ir além do papel e criar, além de rotinas efetivas como: políticas internas, mapeamento de riscos, treinamentos, planos de resposta e auditorias recorrentes, um plano para que haja uma absorção prática, uma conscientização dos colaboradores das empresas para seguirem essas rotinas. No setor financeiro, as normas do BACEN intensificam esse cenário, trazendo exigências detalhadas sobre controles internos, testes de robustez de modelos algorítmicos e integração de compliance de dados à estratégia da empresa (BACEN, 2022)..

2.3.2. Registro de operações de tratamento (ROPA)

As empresas devem manter um registro detalhado das operações de tratamento de dados pessoais, conforme previsto no artigo 37 da LGPD. Este registro deve incluir

finalidade do tratamento, categorias de dados, técnicas aplicadas e procedimentos de segurança e anonimização. No Judiciário, a Resolução CNJ nº 615/2025 exige registros específicos para operações algorítmicas, facilitando auditorias externas e controle social.

2.3.3. Relatório de Impacto à Proteção de Dados (RIPD)

Previsto no artigo 38 da LGPD, o RIPD deve ser elaborado sempre que o tratamento puder gerar riscos relevantes às liberdades individuais. Esse relatório precisa incluir uma avaliação completa dos riscos, descrição das técnicas empregadas, avaliação de proporcionalidade, medidas mitigatórias e explicabilidade dos modelos algorítmicos empregados. Isso inclui, inclusive, a obrigação das empresas, que estiverem em um processo de *M&A*, isto é, de aquisição ou de fusões, de se atentarem aos processos da empresa adquirida ou visada. A Nota Técnica nº 19/2023 da ANPD sugere a integração do RIPD com a Avaliação de Impacto Algorítmico prevista no PL nº 2.338/2023.

2.3.4. Encarregado de Proteção de Dados (DPO)

Toda empresa que trata dados pessoais deve designar um DPO, conforme o artigo 41 da LGPD, responsável por supervisionar o compliance, atender reclamações e atuar como ponto de contato com a ANPD. Em setores altamente regulados, como o financeiro, o DPO é parte integrante da gestão de riscos, reportando diretamente ao comitê de auditoria das instituições financeiras (BACEN, 2022).

2.3.5. Comunicação de incidentes

As empresas devem notificar incidentes de segurança à ANPD em até dois dias úteis, detalhando o incidente, suas consequências potenciais e as medidas corretivas adotadas, conforme a Resolução CD/ANPD nº 15/2024.A falha em comunicar incidentes de segurança no prazo legal constitui infração grave, sujeitando empresas e órgãos públicos a sanções relevantes.

A ANPD, por exemplo, sancionou tanto o INSS quanto a Secretaria de Estado de Educação do Distrito Federal em razão de violações à LGPD, após apuração de vazamentos e de falhas no reporte de incidentes. Os casos em questão, não só apenas reforçam a mudança de um paradigma fiscalizatório e de atuação dos órgãos brasileiros, inclusive dentro da seara pública, como demonstram a importância da comunicação tempestiva e transparente dos

incidentes, bem como da adoção de mecanismos preventivos e corretivos para mitigar danos a titulares e reduzir a responsabilização institucional (ANPD, 2024a; Migalhas, 2024).

2.3.6. Transferências internacionais de dados

Transferências internacionais de dados pessoais são reguladas pelos artigos 33 a 37 da LGPD, sendo permitidas apenas se o país receptor oferecer proteção adequada ou se garantias adicionais forem adotadas, como cláusulas-padrão contratuais aprovadas pela ANPD ou certificações internacionais reconhecidas como o padrão APEC CBPR. Esse requisito é especialmente importante em projetos de IA que dependem de infraestruturas de computação em nuvem estrangeiras.

2.3.7. Uso de Dados Pessoais pela IA

O uso de dados pessoais em sistemas de inteligência artificial apresenta desafios técnicos e regulatórios significativos, especialmente no que se refere à anonimização efetiva dos dados e à prevenção de vieses e discriminação algorítmica. O artigo 20 da LGPD garante aos titulares o direito de solicitar revisão de decisões automatizadas que afetem seus interesses, incluindo a explicação da lógica utilizada pelos algoritmos (Brasil, 2018).

Estudos apontam que modelos de IA frequentemente apresentam vieses decorrentes dos dados utilizados para seu treinamento, o que pode levar à discriminação ilícita ou abusiva. Portanto, torna-se imprescindível implementar processos rigorosos de validação e testes de robustez para minimizar tais riscos, conforme recomendado pela ANPD e normas internacionais como o *AI Act* europeu (União Europeia, 2024).

Entretanto, a efetividade desses dispositivos, presentes na LGPD, por exemplo, ainda depende da consolidação de boas práticas técnicas. Estudos da Fundação Getúlio Vargas (FGV, 2023) e do Instituto de Tecnologia e Sociedade (ITS Rio, 2022) destacam que modelos de IA treinados com datasets históricos tendem a reproduzir padrões de desigualdade, como preconceitos de raça e gênero, o que reforça a necessidade de controles humanos na etapa de curadoria dos dados. O Guia Orientativo de Governança da ANPD (2023) recomenda a implementação de mecanismos de explicabilidade, contestação e supervisão humana, especialmente em decisões de alto impacto.

Outro ponto crítico refere-se à anonimização dos dados pessoais, prevista nos arts. 12 e 13 da LGPD. Embora a anonimização seja uma estratégia relevante para mitigar riscos e retirar os dados do escopo da LGPD, sua efetividade depende da aplicação de técnicas matematicamente sólidas, como *k-anonymity*, *l-diversity* and differential *privacy*, sendo necessário considerar também os riscos de reidentificação por meio de ataques correlacionados (Narayanan; Shmatikov, 2008).

A cadeia de custódia de dados, isto é, a documentação completa de sua origem, manipulação, transformações e uso, é outro requisito essencial para garantir *accountability.* Essa rastreabilidade é um dos pilares do *AI Act* europeu, que classifica sistemas de IA por níveis de risco e impõe deveres de transparência e documentação proporcional à criticidade do modelo (União Europeia, 2024). No Brasil, o PL nº 2.338/2023 avança nessa direção ao prever, nos arts. 25 e 28, obrigações de governança, avaliação de impacto algorítmico e supervisão contínua, criando uma convergência com o regime europeu.

Em projetos que utilizam serviços de nuvem ou fornecedores externos para treinamento de modelos, é imprescindível observar as regras de transferência internacional de dados, conforme arts. 33 a 37 da LGPD, garantindo que os dados estejam sujeitos a padrões de proteção equivalentes, por meio de cláusulas contratuais específicas ou adesão a frameworks reconhecidos nacional ou internacionalmente.

Portanto, o uso de dados pessoais pela IA requer não apenas uma conformidade jurídica ou a criação de documentos dentro de um ambiente corporativo, mas uma governança prática e supervisionada capaz de assegurar a segurança dos direitos fundamentais dos titulares e mitigar riscos sistêmicos, reputacionais e regulatórios.

3. Possíveis Impactos da Regulação de Proteção de Dados e de IA para Operações de M&A no Brasil Envolvendo Empresas de Tecnologia

3.1. A Importância da Due Diligence para a Avaliação de Riscos e Contingências

Operações de *M&A* envolvendo empresas de tecnologia que tratam uma enorme quantidade de dados pessoais e desenvolvem ou utilizam sistemas de IA são cada vez mais comuns no mercado global e nacional. Em nível internacional, vale mencionar três dos maiores *deals* de tecnologia do ano de 2024, envolvendo a aquisição da *Ansys* pela *Synopsys* por *US$* 35 bilhões, da Splunk pela Cisco por *US$* 28 bilhões e da *Juniper Networks* pela HD

por *US$* 14 bilhões (ALI; MARTIN, 2025). Entretanto, transações que envolvem empresas de tecnologia como essas possuem peculiaridades e, por esse motivo, os compradores e os vendedores, orientados por seus respectivos assessores, devem adotar certas medidas para mitigar riscos regulatórios, em todas as etapas desse processo.

A *due diligence* é uma fase essencial para qualquer processo de *M&A*. É ela que permite, a partir da análise dos documentos e informações disponibilizados ao potencial comprador ou publicamente, identificar os riscos inerentes à sociedade e/ou ao ativo alvo (*target*), incluindo suas contingências materializadas e não materializadas, relacionadas ou não ao cumprimento da estrutura regulatória aplicável. Os resultados de uma *due diligence,* abrangente ou mais limitada, geralmente são incorporados nos documentos definitivos da operação, por meio de cláusulas de declarações e garantias e de indenização, como será explorado no item seguinte, ou na precificação do *target.*

A amplitude de cada *due diligence* depende da dimensão da operação a que ela se destina (RAUPP; WARKEN, 2009). Nesse sentido, enquanto os assessores de operações que envolvem um *valuation* mais baixo tendem a adotar um escopo bastante limitado para essa investigação, com foco nas áreas críticas e que possuem maior risco de sucessão empresarial, como trabalhista, fiscal e previdenciária, geralmente se baseando em documentos tornados públicos pela *target* (*high level due diligence*), um *M&A* com *ticket* mais elevado tende a requerer uma análise bastante detalhada e completa da documentação específica da empresa e/ou ativo alvo, sob a perspectiva de todas as possíveis áreas relacionadas (*full blown due diligence*). Importante ressaltar, ainda, que a *due diligence* pode ser conduzida por diversos assessores do potencial comprador ao mesmo tempo, do ponto de vista legal, operacional, técnico, financeiro, dentre outros.

Nos casos em que a empresa *target* desenvolve atividades relacionadas a tecnologia e inovação, a *due diligence* jurídica precisa considerar sua adequação ao arcabouço regulatório aplicável sobre proteção de dados pessoais e inteligência artificial, descrito de forma detalhada nos capítulos acima. Nesse sentido, os assessores do possível comprador devem avaliar com atenção a existência do RIPD da empresa alvo e, em caso positivo, se seus termos estão adequados à LGPD e às demais regras nacionais e internacionais aplicáveis, além da eventual entrega de documentos tempestiva sobre o tema para as autoridades governamentais competentes (COELHO, 2023).

Como destaca Cavalcante (2024, p. 23-24), o avanço acelerado da IA acarreta desafios técnicos e éticos, como a opacidade dos sistemas e a dificuldade de supervisão humana, o que intensifica os riscos e preocupação durante o processo de *due diligence*, a falta de interoperabilidade dos sistemas, a discriminação algorítmica e a opacidade das máquinas torna mais difícil a supervisão humana e a responsabilização por danos causados por essa estrutura.

Além disso, é importante que se faça uma avaliação sobre o grau de risco - conforme atribuído pelas normas internacionais aplicáveis e, caso aprovado, pelo PL 2.338/2023 - de seus sistema de inteligência artificial, caso a *target* seja um fornecedor desse tipo de tecnologia.

Sendo assim, eventuais descobertas de falhas durante a *due diligence* de uma operação podem gerar impactos negativos para o *valuation* da empresa alvo e sua imagem no mercado, considerando as informações obtidas por potenciais investidores. Por outro lado, os compradores que negligenciam essa investigação podem também sofrer danos reputacionais e precisar arcar com contingências não esperadas resultantes da sucessão empresarial, uma vez que não foram endereçadas nos documentos aplicáveis considerando a devida proteção ao investidor (BARBOSA, 2025).

A relevância da condução de uma *due diligence* jurídica atenta e compreensiva em um processo de *M&A* envolvendo empresas de tecnologia já mostrou seus efeitos práticos em casos concretos. Vale citar um exemplo que envolveu duas gigantes da tecnologia: Yahoo, como *target,* e Verizon, como sua adquirente. Em 2017, assinaram os documentos da operação que teve seu valor reduzido em aproximadamente US$ 350 milhões pela compradora em razão da descoberta, após a conclusão da *due diligence*, de ataques cibernéticos e vazamento de dados envolvendo a Yahoo (ATHAVALEY; SHEPARDSON, 2017).

3.2. Cláusulas de Declarações e Garantias e de Indenização

Conforme mencionado no item acima, uma das principais formas de afastar a contaminação da compradora pelas contingências relacionadas à inobservância da regulação é a inclusão de cláusulas de declarações e garantias (*representations and warranties*) e de indenização, que estão intimamente relacionadas, nos documentos definitivos que regerão as

operações, os quais geralmente assumem a forma de contrato de compra e venda de ações ou quotas ou de acordo de investimento.

Como ensina a professora Caitlin Mulholland:

> As cláusulas de declarações e garantias encontram origem na *common law* configuram declarações expressas emitidas pelas partes contratantes no corpo de um contrato, visando o reconhecimento de determinadas informações pretéritas ou presentes a respeito de condições essenciais para a formação e execução de um negócio jurídico (MULHOLLAND, 2022)

Sendo assim, elas estão atreladas à boa-fé e ao dever de informar (DE CASTRO *et al,* 2023) e servem para refletir a imagem da empresa alvo no momento da conclusão da *due diligence*, devendo indicar, inclusive, todas as contingências e falhas identificadas pelos consultores durante esse processo.

Dessarte, presume-se que o comprador teve acesso a todas as informações relevantes e, principalmente, as que podem gerar impactos negativos para o investidor e apresentou sua oferta informada com base nos riscos identificados durante essa análise. Caso isso não se mostre verdadeiro, o comprador pode ser ressarcido pelos eventuais danos sofridos em razão de passivos, incluindo multas e penalidades administrativas aplicadas pelo descumprimento da regulação.

Isso porque é comum que as partes contratantes estabeleçam, nos documentos definitivos da operação, que as hipóteses de falsidade, incompletude, inexatidão e/ou omissão relacionada às declarações e garantias prestadas pela *target* obriguem os vendedores e/ou a empresa alvo, individual ou solidariamente, a indenizar a compradora por eventuais perdas e danos decorrentes desse fato. Ademais, também é usual que, de forma mais abrangente, as partes determinem que os vendedores e/ou a *target* devem indenizar a compradora por prejuízos resultantes quaisquer atos ou fatos cujo fato gerador tenha ocorrido até o fechamento da compra e venda (FREITAS, 2020).

Diante da evolução tecnológica, cláusulas de declarações e garantias que indiquem a adequação da *target* às normas aplicáveis sobre proteção de dados pessoais e sistemas de inteligência artificial são cada vez mais comuns. Nesse sentido, os compradores podem exigir que a empresa alvo declare que cumpre com as regras cabíveis no tratamento de dados pessoais por ela coletados, seja por meio de IA ou não, que possui as licenças adequadas e/ou

a propriedade dos produtos de IA por ela desenvolvidos ou fornecidos e que realiza monitoramento frequente desses sistemas, dentre outros aspectos de conformidade (CHOUDHRY et al, 2025).

Não obstante, é inegável a rapidez das mudanças regulatórias que ocorrem em relação aos temas de proteção de dados pessoais e desenvolvimento e uso de IA. Nesse sentido, é importante que as cláusulas sejam redigidas pensando em uma possível evolução do arcabouço legal e que as declarações ali prestadas podem rapidamente tornar-se imprecisas ou equivocadas.

3.3. Condições Precedentes dos Contratos Definitivos

Conforme mencionado acima, a regulação de proteção de dados pessoais e inteligência artificial no Brasil está em constante evolução e, por isso, precisa ser acompanhada de perto por aqueles que podem ser por ela afetados. Nesse sentido, caso os compradores não se sintam confortáveis em concluir a compra e venda da empresa alvo antes que ela esteja plenamente adequada às normas sobre esses temas então vigentes, é possível incluir uma condição precedente nos documentos definitivos da transação com tal finalidade.

Como observa Cavalcante (2024), o desenvolvimento e uso de sistemas inteligentes, seja no setor público ou privado, demanda um marco regulatório que vá além da técnica. "É imprescindível considerar valores como transparência, *accountability* e diversidade para mitigar riscos éticos e garantir decisões justas e auditáveis" (CAVALCANTE, 2024, p. 28-30). A incorporação desses princípios nas condições precedentes pode, portanto, proteger os adquirentes diante de falhas estruturais nos sistemas algorítmicos utilizados pela empresa alvo.

A doutrina discute se essa cláusula possui natureza resolutiva ou suspensiva, nos termos dos artigos 124 e seguintes do Código Civil Basileiro (L'APICCIRELLA, 2022). Entretanto, não há dúvidas de que ela condiciona o fechamento (*closing*) da operação ao cumprimento de determinados atos a serem observados pela *target* ou obtidos de credores, autoridades governamentais ou outros terceiros. Essas condições precisam ser comprovadamente satisfeitas, mas também podem ser dispensadas, a critério dos vendedores, de acordo com as disposições que forem incluídas com tal finalidade nos documentos definitivos da transação.

Nesse sentido, a título exemplificativo, é possível que os compradores solicitem a inclusão de uma cláusula que dispõe que a empresa alvo deve realizar o mapeamento do seu tratamento de dados pessoais e a elaboração de um RIPD, a ser disponibilizado de forma facilitada aos titulares e publicado mediante determinação da ANPD (ANPD, 2023). Além disso, o comprador poderia exigir que a empresa alvo elaborasse Políticas de *Compliance* e Privacidade, como condição para o pagamento do valor devido aos vendedores e, consequentemente, para o fechamento.

Outra cláusula bastante comum nos contratos de compra e venda de ativos e que pode endereçar a preocupação de observância regulatória de outra modalidade é a dos atos de fechamento. Diferentemente das condições precedentes, ela não impede a concretização do negócio até o seu efetivo cumprimento, mas sim, diz respeito a atos que devem ser praticados e documentos que devem ser apresentados aos compradores até ou na data do *closing,* sob pena de descumprimento contratual.

Conclusão

Não há dúvidas de que empresas que tratam uma imensa base de dados pessoais de clientes, fornecedores e terceiros e que estão engajadas com o desenvolvimento e a exploração de sistemas de IA são cada vez mais visadas no mercado de *M&A* do Brasil e do mundo, afinal, conforme popularizado pelo matemático britânico Clive Humby, "*dados são o novo petróleo*".

Além disso, todas as indústrias estão interessadas em otimizar os seus negócios com o uso de IA. Atualmente, o emprego de soluções inovadoras que otimizam resultados e reduzem custos é um diferencial no mercado, o que leva multinacionais e grandes empresas e adquirem *startups* e novos empreendimentos que possuem capital intelectual para o desenvolvimento desses sistemas, aumentando sua eficiência e competitividade em um contexto mercadológico que está em constante evolução (NOBILE, 2025).

Entretanto, tendo em vista que o arcabouço regulatório envolvendo novas tecnologias, especialmente no que diz respeito à proteção dos dados pessoais tratados por esses sistemas e à IA, é rapidamente modificado e atualizado, os interessados nas operações precisam estar atentos a determinadas peculiaridades envolvendo essas empresas alvo, a fim de mitigar

eventuais riscos regulatórios, jurídicos e de *compliance* (BROADBENT; REHAAG, 2025). Além disso, tais cuidados podem ser necessários para evitar a contaminação dos compradores com penalidades administrativas que venham a ser eventualmente aplicadas por autoridades como a ANPD pelo descumprimento das regras aplicáveis.

Nesse sentido, conforme exposto acima, os potenciais investidores e vendedores precisam contratar cuidadosamente assessores jurídicos, financeiros e técnicos que possam auxiliá-los não apenas a moldar cláusulas contratuais que enderecem esses riscos, seja no formato de de declarações e garantias, indenizações e/ou condições precedentes, mas também a fazer uma completa auditoria da *target*, que os permita ter clareza sobre as lacunas e problemas de fato existentes - e que devem impactar diretamente a negociação.

Contudo, não se tratam de resultados estáticos. Como exposto nos Capítulos 2 e 3 acima, a regulação de proteção de dados pessoais e IA no Brasil ainda é incipiente e, em relação a certos pontos, inexistente, estando apenas no formato de projetos de lei. Sendo assim, as nuances de sua efetiva aplicação ainda serão descobertas pelo mercado. Por esse motivo, a análise de riscos regulatórios relacionada a esses temas é fluída e deve ser atualizada constantemente, acompanhando-se de perto as discussões das autoridades legislativas e administrativas no Brasil e no mundo. Afinal, como identificado em relatório da [Deloitte], no que diz respeito à indústria ora analisada, destacar-se-ão aqueles que conseguem navegar novos desafios e se adaptar rapidamente a eles (DELOITTE, 2024).

Referências Bibliográficas

AGÊNCIA SENADO. **Comissão temporária debate efeitos da inteligência artificial nos direitos fundamentais do titular de dados pessoais**. 2023. Disponível em: https://agenciadenoticias.senado.leg.br/noticia/comissao-temporaria-de-ia-debate-efeitos. Acesso em: 26 jul. 2025.

AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA (ANVISA). **Resolução RDC nº 657, de 24 de fevereiro de 2022.** Disponível em: https://www.gov.br/anvisa/pt-br/assuntos/produtosparasaude/temas-em-destaque/arquivos/2024/rdc-657-2022-en.pdf. Acesso em: 26 jul. 2025.

ALIANT; PROTIVITI. 2ª Pesquisa nacional sobre as necessidades e tendências em Compliance, 2025. Disponível em: https://conteudos.aliant.com.br/lp-tendencias-em-compliance-2025. Acesso em: 20 jul. 2025.

ALI, Faria; MARTIN, Roddy. ***Global M&A Report 2025: sector and broader perspectives. AI and M&A – What you need to know***. Herberth Smith Freehills Kramer, 2025. Disponível em: https://www.hsfkramer.com/insights/reports/2025/global-ma-report-2025/sector-and-broader-perspectives/ai-and-m-and-a—what-you-need-to-know . Acesso em: 27 jul. 2025.

ATHAVALEY, Anjali; SHEPARDSON, David. ***Verizon, Yahoo agree to cut deal price by US$ 350 million***. Yahoo Finance, 2017. Disponível em: https://finance.yahoo.com/news/verizon-yahoo-agree-cut-deal-price-much-350-123807895--finance.html. Acesso em: 25 jul. 2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS**. Perguntas e respostas sobre o Relatório de Impacto à Proteção de Dados Pessoais**. 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 27 jul. 2025.

BARBOSA, Paulo**. *Cyber due diligence* em fusões e aquisições**. São Paulo: Instituto Brasileiro de Governança Corporativa, 2025. Disponível em: https://www.ibgc.org.br/blog/artigo-cyber-due-diligence. Acesso em: 26 jul. 2025.

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: Data Privacy Brasil, 2023. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2023/12/dataprivacy_nota-tecnica-temas-regulatorios.pdf. Acesso em: 27 jul. 2025.

BOSTON CONSULTING GROUP. *The payoffs and pitfalls of ESG due diligence*. Boston: BCG, 2024. Disponível em: https://www.bcg.com/publications/2024/payoffs-and-pitfalls-of-esg-due-diligence. Acesso em: 20 jul. 2025.

BRASIL. **Estratégia Brasileira de Inteligência Artificial (EBIA).** Brasília: Ministério da Gestão e da Inovação em Serviços Públicos, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/estrategia-brasileira-de-inteligencia-artificial. Acesso em: 26 jul. 2025.

BRASIL. **Lei nº 14.460, de 25 de outubro de 2022**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14460.htm. Acesso em: 26 jul. 2025.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13853.htm. Acesso em: 26 jul. 2025.

BRASIL. Agência Nacional de Proteção de Dados. ANPD sanciona INSS e Secretaria de Educação do DF por violações à LGPD. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-sanciona-inss-e-secretaria-de-educacao-do-df-por-violacoes-a-lgpd. Acesso em: 27 jul. 2025.

CAVALCANTE, Jamile Sabbad Carecho. *Inteligência Artificial nos Tribunais: desafios éticos e jurisdição*. Londrina: Thoth, 2024.

CeMEAI/USP. **Comissão Temporária de IA debate os efeitos da inteligência artificial nos direitos fundamentais do titular de dados pessoais**. 2023. Disponível em: https://cemeai.icmc.usp.br/comissao-temporaria-de-ia-debate-os-efeitos-da-inteligencia-artificial-nos-direitos-fundamentais-do-titular-de-dados-pessoais/. Acesso em: 26 jul. 2025.

CENTRAL DO VAREJO. Possível cisão de Arezzo e Grupo Soma causa queda de 10 % nas ações de conglomerado. 18 mar. 2025. Disponível em: https://centraldovarejo.com.br/possivel-cisao-de-arezzo-e-grupo-soma-causa-queda-de-10-nas-acoes-de-conglomerado/. Acesso em: 20 jul. 2025.

CHOUDRY, Mavra et al. ***Acquiring AI: Considerations for representations and warranties in transaction documents.*** Torys LLP, 2025. Disponível em: https://www.torys.com/our-latest-thinking/publications/2025/03/considerations-for-representations-and-warranties-in-transaction-documents. Acesso em: 25 jul. 2025.

COELHO, Alexander. **A proteção de dados nos processos de *due diligence*.** Migalhas, 2023. Disponível em: https://www.migalhas.com.br/depeso/381346/a-protecao-de-dados-nos-processos-de-due-diligence. Acesso em: 25 jul. 2025.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). **Instrução nº 626, de 15 de maio de 2020**. Disponível em: https://conteudo.cvm.gov.br/legislacao/instrucoes/inst626.html. Acesso em: 26 jul. 2025.

COMISSÃO DE VALORES MOBILIÁRIOS (CVM). **Resolução nº 29, de 11 de maio de 2021**. Disponível em: https://conteudo.cvm.gov.br/legislacao/resolucoes/resol029.html. Acesso em: 26 jul. 2025.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução nº 615, de 14 de junho de 2024**. Disponível em: https://atos.cnj.jus.br/files/original155530202503146 7d4517244566.pdf. Acesso em: 26 jul. 2025.

CORRIGAN, Jack; LUONG, Ngor; SCHOEBERL, Christian. ***Acquiring AI companies: Tracking U.S. AI mergers and acquisitions.*** Georgetown CSET, 2024. Disponível em: https://cset.georgetown.edu/publication/acquiring-ai-companies-tracking-u-s-ai-mergers-and-acquisitions/. Acesso em: 27 jul. 2025.

DATA PRIVACY BRASIL. **Contribuições do Data Privacy Brasil ao Projeto de Lei nº 21, de 4 de fevereiro de 2020.** São Paulo, 2021. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2021/09/dpbr_notatecnica_pl21.pdf. Acesso em: 26 jul. 2025.

DATA PRIVACY BRASIL. **Temas centrais na regulação de IA: inteligência artificial e proteção de dados.** São Paulo, 2023. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2023/12/dataprivacy_nota-tecnica-temas-regulatorios.pdf. Acesso em: 26 jul. 2025.

DATA PRIVACY BRASIL. **A construção da legislação de Inteligência Artificial no Brasil: análise técnica do texto que será votado no Plenário do Senado Federal**. São Paulo, 2024. Disponível em: https://www.dataprivacybr.org/documentos/a-construcao-da-legislacao-de-inteligencia-artifici

al-no-brasil-analise-tecnica-do-texto-que-sera-votado-no-plenario-do-senado-federal/. Acesso em: 26 jul. 2025.

DELOITTE. ***Artificial intelligence and mergers and acquisitions: Observations from the frontlines and how to prepare for the coming shift***. 2024. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/mergers-acqisitions/us-artificial-intelligence-and-mergers-and-acquisitions.pdf. Acesso em: 27 jul. 2025.

DONEDA, Danilo. **Responsabilidade e transparência algorítmica na inteligência artificial**. In: GAMBA, S. R. H. (Org.). Ciência, Tecnologia e Inovação na Governança da IA. Série Engenharias. Atena Editora, 2025. Disponível em: https://atenaeditora.com.br/index.php/catalogo/dowload-post/97317. Acesso em: 26 jul. 2025.

FREITAS, Bernardo. **Decisão do TJSP destaca importância da cláusula de indenização em operações de *M&A***. Legislação & Mercados (Capital Aberto), 2020. Disponível em: https://legislacaoemercados.capitalaberto.com.br/decisao-do-tjsp-destaca-importancia-da-clausula-de-indenizacao-em-operacoes-de-ma/. Acesso em: 25 jul. 2025.

GOULART, Guilherme Damasio. **Comentários à Lei Geral de Proteção de Dados**. In: MARTINS, G. M.; LONGHI, J. V. R.; FALEIROS JÚNIOR, J. L. M. (Orgs.). Indaiatuba, SP: Editora Foco, 2022. p. 268-269. Disponível em: https://site.conpedi.org.br/publicacoes/pxt3v6m5/7v339923/naN70S8tgYMQBPn2.pdf. Acesso em: 26 jul. 2025.

INVESTALK. Azzas nega rumores sobre fim da parceria entre Arezzo e Soma; divergências são antigas. 19 mar. 2025. Disponível em: https://investalk.bb.com.br/noticias/mercado/azzas-nega-rumores-sobre-fim-da-parceria-entre-arezzo-e-soma-divergencias-sao-antigas. Acesso em: 20 jul. 2025.

KPMG. *KPMG global tech report 2024 – Beyond the hype: balancing speed, security and value*. Amsterdã: KPMG International, 2024. Disponível em: https://kpmg.com/xx/en/our-insights/transformation/kpmg-global-tech-report-2024.html . Acesso em: 20 jul. 2025.

LEXISNEXIS RISK SOLUTIONS; FORRESTER CONSULTING. O real custo do compliance contra crimes financeiros – América Latina, 2024. Disponível em: https://www.prnewswire.com/br/comunicados-para-a-imprensa/estudo-revela-que-o-custo-anual-do-compliance-contra-crimes-financeiros-totaliza-us-15-bilhoes-na-america-latina-302118039.html. Acesso em: 20 jul. 2025.

L'APICCIRELLA, Danielli Gilbert de Souza. **O processo de negociação em projetos de fusões e aquisições, sob a ótica da advogada jurídica corporativa de indústria: melhores práticas e patologias.** São Paulo: Fundação Getúlio Vargas, 2022. Disponível em: https://direitosp.fgv.br/sites/default/files/arquivos/232.pdf. Acesso em: 27 jul. 2025.

MACHADO MEYER ADVOGADOS. **Panorama regulatório da saúde digital no Brasil**. São Paulo, 2024. Disponível em: https://www.machadomeyer.com.br/images/ebooks/Regulacao_saude_Digital_2024.pdf. Acesso em: 26 jul. 2025.

MIGALHAS. ANPD condena INSS por vazamento de dados. 2024. Disponível em: https://www.migalhas.com.br/quentes/401393/anpd-condena-inss-por-vazamento-de-dados. Acesso em: 27 jul. 2025.

MULHOLLAND, Caitlin. **As cláusulas de declarações e garantias e a aplicação do princípio da boa-fé objetiva nos contratos societários.** Rio de Janeiro/RJ. 2022. Pág. 1. Disponível em https://www.jur.puc-rio.br/wpcontent/uploads/2022/08/Texto-9.pdf. Acesso em 24/07/25.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *Global Trends in Government Innovation 2023*. Paris: OECD Publishing, 2023. Disponívelem:https://www.oecd.org/en/publications/global-trends-in-government-innovation-2023_0655b570-en.html. Acesso em: 20 jul. 2025.

RAUPP, Fabiano Maury; WARKEN, Ricardo Muller. **Utilização da *due diligence* em processos de fusão e aquisição**. In Pensar Contábil, Vol. 11, No. 45. 2009. Disponível em: http://www.atena.org.br/revista/ojs-2.2.3-06/index.php/pensarcontabil/article/view/136. Acesso em: 26 jul. 2025.

RODRIGUES, Carla; MENDONÇA, Eduardo; NÓVOA, Natasha. **IA e as mudanças no judiciário brasileiro.** São Paulo: Data Privacy Brasil, 2025. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2025/03/IA-e-as-mudancas-no-judiciario-brasileiro-Data-Privacy-Brasil.pdf. Acesso em: 26 jul. 2025.

SAGAR, Kuldeep. Invisible threats: why cybersecurity due diligence is non-negotiable in M&A. *Reuters Legal*, Nova Iorque, 24 jan. 2025. Disponível em: https://www.reuters.com/legal/transactional/invisible-threats-why-cybersecurity-due-diligence-is-nonnegotiable-ma-2025-01-24/. Acesso em: 20 jul. 2025.

SENADO FEDERAL. **Atividades legislativas: audiências públicas realizadas, composição e tramitação do PL 2338/2023**. Brasília: Comissão Temporária Interna sobre Inteligência Artificial no Brasil, 2023-2024. Disponível em: https://legis.senado.leg.br/atividade/comissoes/comissao/2629. Acesso em: 26 jul. 2025.

SENADO FEDERAL. **Projeto de Lei nº 2.338, de 2023.** Brasília: Senado Federal, 2024-2025. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233 . Acesso em: 26 jul. 2025.

UNITED STATES OF AMERICA. ***Executive Order 14110: Safe, Secure, and Trustworthy Artificial Intelligence***. Washington DC, 2023. Disponível em: https://www.govinfo.gov/content/pkg/DCPD-202300949/pdf/DCPD-202300949.pdf. Acesso em: 26 jul. 2025.

VIEIRA, James Batista et al. **O *sandbox* regulatório como instrumento de incentivo à inovação no Brasil: os casos do Banco Central do Brasil, da Comissão de Valores Mobiliários e da Superintendência de Seguros Privados**. Revista do TCU, Brasília, v. 153, n. 1, p. 336-362, 2024. Disponível em: https://doi.org/10.69518/RTCU.153.336-362. Acesso em: 27 jul. 2025.