IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO EMPRESARIAL

JEFFERSON APARECIDO DIAS

VIVIANE COÊLHO DE SÉLLOS KNOERR

LUCIANE APARECIDA FILIPINI STOBE

Copyright © 2026 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI
Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU – São Paulo
Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina
Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa – Pará
Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG – Goiás
Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul
Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio – Rio de Janeiro
Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:
Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão
Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais
Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte
Prof. Dr. Fernando Passos – UNIARA - São Paulo
Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo
Secretarias
Relações Institucionais:
Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná
Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia
Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal
Comunicação:
Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina
Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul
Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe
Relações Internacionais para o Continente Americano:
Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do sul
Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão
Prof. Dr. Felipe Chiarello de Souza Pinto - UPM – São Paulo
Relações Internacionais para os demais Continentes:
Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará
Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul
Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI – Santa Catarina
Educação Jurídica
Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR
Prof. Dr. Rubens Beçak - USP - SP
Profa. Dra. Livia Gaigher Bosio Campello – UFMS – MS
Eventos:
Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo
Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina
Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial
Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ
Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB
Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG
Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito empresarial [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Jefferson Aparecido Dias; Viviane Coêlho de Séllos Knoerr; Luciane Aparecida Filipini Stobe – Florianópolis: CONPEDI, 2026.

Inclui bibliografia
ISBN: 978-65-5274-605-4
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Empresarial. 2. Direito civil. 3. Contemporâneo. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO EMPRESARIAL

Apresentação

Honrados, apresentamos os trabalhos defendidos durante o IX Encontro Virtual do CONPEDI, no âmbito do GT 63 - Direito Empresarial. Temas variados foram abordados, todos envolvendo os desafios da governança corporativa na contemporaneidade, os quais agora são apresentados ao leitor.

Raquel Xavier Vieira Braga, Luciano Rosa Vicente e Liziane Paixão Silva Oliveira analisaram a efetividade do sistema de prevenção do cyber trading, com o objetivo de verificar se há capacidade do poder judiciário de coibi-lo.

Rogério Mello, Arthur Guedes da Fonseca Mello e Fernando Antônio Nunes Ferreira fizeram uma análise do conflito normativo empresarial, visando os termos de nulidade de acordo privado, ante a vedação do reajuste infra anual.

Jaqueline de Oliveira Arruda, Jefferson Aparecido Dias e Giowana Parra Gimenes da Cunha, ao desenvolverem o estudo intitulado “Governança corporativa e compliance como limite ao fomento de torcidas organizadas (TO’s): uma análise do compliance desportivo e o caso da Sociedade Esportiva Palmeiras”, demonstraram formas de implementação da governança corporativa e do compliance e como os clubes de futebol, especialmente a Sociedade Esportiva Palmeiras, podem utilizar dessas ferramentas para aperfeiçoar as gestões junto as torcidas organizadas.

Carolina Reco dos Santos, Diego Cesar Santana e Luis Hilário Tobler Garcia desenvolveram o artigo nomeado “Governança jurídica da inteligência artificial nas organizações: o papel do

Carlos Alberto Martins Junior, no estudo “Patrimônio de afetação na incorporação imobiliária: incomunicabilidade patrimonial e incompatibilidade com a recuperação judicial do incorporador”, explorou as possibilidades de o patrimônio de afetação vinculado à incorporação imobiliária ser ou não alcançado pelos efeitos da recuperação judicial do incorporador.

Suelaine Pacheco Dantas de Alencar e Estevan Lo Ré Pousada desenvolveram uma análise sobre a “Gestão de riscos, desequilíbrio na execução contratual e o dever de renegociação: quando a vida real desafia o mundo ideal previsto no contrato empresarial”, com objetivo de compreender a função social e o equilíbrio contratual, diante dos desafios supervenientes impostos pela realidade durante a execução dos contratos empresariais.

Andressa Juliana Alexandre Pedrochi Alves Feitoza e Andryelle Vanessa realizaram duas análises. A primeira sendo da “Tutela da personalidade post mortem em plataformas digitais: instrumentos de efetivação para gestão da herança digital”, com foco na sucessão dos bens imateriais e híbridos, com a conclusão de que o trato dos bens digitais não pode ser encarada como mercadoria e sim como extensão da personalidade. O segundo estudo foi o “Compromisso de compra e venda e a função social do contrato: reflexos na tutela dos direitos da personalidade do consumidor”, no qual dialogaram com a natureza híbrida dos direitos do consumidor, compreendendo a relação entre o Código de Defesa do Consumidor e o Código Civil.

Tathyana Froes Diogo André e Leonardo da Silva Sant Anna, no artigo intitulado “A responsabilidade do sócio cedente na sociedade limitada: limites interpretativos dos arts. 1003, parágrafo único, e 1032 do Código Civil”, exploraram os limites da responsabilização social do sócio cedente.

Diego Roberto Pinheiro Ferreira, no ensaio “DIP Financing e marco legal das garantias:

Miriam da Costa Claudino, Alexandre Eli Alves e Ricardo Augusto Bonotto Barboza, na pesquisa nomeada “A evolução dos contratos de vesting nas Biostartups: uma análise da boa-fé contratual”, exploraram a necessidade normatização adequada, com foco na boa-fé contratual.

Rafael Lima Carvalho e Pedro Durão, no artigo “Ética empresarial, dever de informação e sigilo profissional: um estudo sobre o papel da empresa na proteção de direitos fundamentais”, pesquisaram sobre a prevenção e compromisso ético das empresas para além das sanções judiciais eventualmente impostas por atos reprováveis.

Laura Gripp Rosas e Elcio Nacur Rezende, no estudo “O compliance contaminado: polarização política, governança e a crise da agenda anticorrupção empresarial”, analisaram como os programas de compliance devem estar acima da polarização política de que os gestores e/ou donos possam estar contaminados.

Tânia Zuily Cabral Vitamatos e Daniel Alves Aragão de Seixas, com o ensaio “A arquitetura jurídica dos empreendimentos de solidariedade e o art. 170: governança participativa, função social da empresa e tensões regulatórias no espaço urbano de São Paulo”, buscaram compreender que a arquitetura brasileira não é limitada apenas na busca do lucro, incluindo a função social das empresas como mais um polo norteador.

Matheus Victor Soligueti Bezerra e Rafael Mercadante Junior, no estudo “Responsabilidade por omissão dolosa nas declarações e garantias dos contratos de aquisição societária: limites e implicações da cláusula de Sandbagging”, buscaram entender até que ponto o vendedor pode ser responsabilizado pela omissão, mesmo com aplicação do due diligence por parte do comprador.

Ana Clara Vasques Gimenez, Matheus Arcoleze Marelli e Elaine Cristina Vieira Brandão, no

Daniel Bushatsky e Marcio Rodrigues, na pesquisa “Da segurança digital à segurança jurídica: custódia de dados, LGPD e prova digital em pequenos e médios e-commerces”, analisaram a possibilidade de proteção dos pequenos e médios empreendedores ante a capacidade probatória durante a fase de instrução.

Carla Izolda Fiuza Costa Marshall, Guilherme Fabbriziani Borges e Matheus Marques de Albuquerque, no estudo intitulado “Análise econômica do direito, consequencialismo jurídico e impactos sobre os stakeholders: reflexões sobre o devedor contumaz”, discutiram os impactos jurídicos e econômicos decorrentes da atuação do devedor contumaz, buscando compreender a extensão de seus efeitos sobre as empresas em situação de crise e sobre os demais stakeholders envolvidos.

Davi Niemann Ottoni, Matheus Oliveira Maia e Claudiomar Vieira Cardoso, no estudo “Modernidade tecnológica, inteligência artificial e direitos fundamentais: desafios jurídicos do desenvolvimento social na sociedade digital”, debruçaram-se sobre a tendência absoluta do mercado com a utilização das inteligências artificiais, entendendo que a I.A. é uma ferramenta que deve ser operada com supervisão humana.

Gabriel Magalhães Comegno, no ensaio “Direitos essenciais dos acionistas e a possibilidade de suspensão de seu exercício”, explorou os limites de suspensão dos poderes dos acionistas, ante o conceito de essencialidade.

Letícia Rosim, Fernando Passos e Fernando Henrique Rugno da Silva, na pesquisa intitulada “Turnaround empresarial, governança e gestão de conflitos na reestruturação de empresas em crise financeira”, exploraram a aproximação do meio jurídico com o turnaround administrativo.

Álvaro dos Santos Maciel e Saulo Bichara Mendonça, no estudo do “Compliance na pequena empresa: entre o cosmético e o efetivo”, estudaram a possibilidade da implementação do

Prof.ª Dra. Luciane Aparecida Filipini Stobe (UNOCHAPECO)

Prof. Dr. Jefferson Aparecido Dias (UNIMAR)

GOVERNANÇA JURÍDICA DA INTELIGÊNCIA ARTIFICIAL NAS ORGANIZAÇÕES: O PAPEL DO GESTOR COMO AGENTE DE CONFORMIDADE DIGITAL

LEGAL GOVERNANCE OF ARTIFICIAL INTELLIGENCE IN ORGANIZATIONS: THE ROLE OF MANAGERS AS AGENTS OF DIGITAL COMPLIANCE

Carolina Reco dos Santos
Diego Cesar Santana
Luis Hilario Tobler Garcia

Resumo

O presente artigo analisa os desafios jurídicos e gerenciais decorrentes da adoção de sistemas de Inteligência Artificial (IA) pelas organizações. O estudo fundamenta-se em marcos regulatórios contemporâneos, como o EU AI Act, que estabelece obrigações proporcionais ao nível de risco dos sistemas e cuja entrada em vigor está prevista para 2026, bem como em padrões internacionais de governança, como a ISO/IEC 42001:2023, que orienta a estruturação de processos organizacionais para o uso responsável da IA. No contexto brasileiro, examina-se o Projeto de Lei nº 2.338/2023, já aprovado pelo Senado Federal e em tramitação na Câmara dos Deputados, que adota abordagem baseada em risco, com ênfase na transparência, na mitigação de danos e na proteção de direitos fundamentais. Além disso, o artigo utiliza frameworks de gestão de riscos, como o NIST AI RMF 1.0, e princípios internacionais, como os OECD AI Principles, que tratam de transparência, segurança e responsabilidade no uso da IA. O objetivo é demonstrar o papel central do gestor como agente de conformidade digital, responsável por traduzir exigências legais em práticas organizacionais, incluindo identificação de sistemas, avaliação de riscos, supervisão humana, monitoramento de impactos e resposta a incidentes.

Palavras-chave: Inteligência artificial, Governança de ia, Conformidade digital, Gestão de riscos, Responsabilidade

Abstract/Resumen/Résumé

the NIST AI RMF 1.0 and international principles such as the OECD AI Principles, which address transparency, safety, and accountability in the use of AI. The objective is to demonstrate the central role of managers as agents of digital compliance, responsible for translating legal requirements into organizational practices, including system identification, risk assessment, human oversight, impact monitoring, and incident response.

Keywords/Palabras-claves/Mots-clés: Artificial intelligence, Ai governance, Digital compliance, Risk management, Accountability

INTRODUÇÃO

O objeto geral deste estudo é analisar como Inteligência Artificial (IA) tornou-se um dos elementos mais marcantes da transformação digital contemporânea, influenciando tanto processos corporativos quanto decisões tomadas por órgãos públicos. Atualmente empresas utilizam IA para análise de dados, seleção de candidatos, detecção de fraudes, recomendação de produtos e gestão de riscos; governos adotam sistemas automatizados para otimizar políticas públicas, administrar serviços, apoiar decisões judiciais ou analisar benefícios sociais. Esse movimento já é observado em escala global, inclusive por organizações internacionais que monitoram o uso crescente de IA em diversas funções públicas e privadas.

A crescente adoção da Inteligência Artificial se deve a promessa de eficiência, precisão e economia de recursos, proporcionando respostas rápidas para problemas complexos. Porém, junto aos benefícios surgem riscos significativos e um dos principais desafios é a chamada opacidade algorítmica, que descreve a dificuldade de compreender como sistemas automatizados chegam às suas conclusões, especialmente modelos avançados de aprendizado de máquina, cujo funcionamento interno nem sempre é interpretável. Além disso, sistemas de IA podem reproduzir ou ampliar vieses discriminatórios presentes nos dados de treinamento, afetando decisões de grande impacto humano, como concessão de crédito, triagem de currículos ou definição de políticas públicas. A literatura internacional destaca ainda perigos relacionados à segurança da informação, uma vez que modelos podem ser vulneráveis a ataques, e à proteção de dados pessoais, tema sensível para a sociedade contemporânea. Tais preocupações são reconhecidas em marcos internacionais, como os Princípios de IA da OCDE, que defendem transparência, responsabilidade e mitigação de riscos.

Diante desses riscos, o desenvolvimento de um marco regulatório robusto tornou-se essencial. No Brasil, a Lei Geral de Proteção de Dados (LGPD) já estabelece princípios relevantes para o tratamento de dados pessoais, que se aplicam diretamente ao funcionamento de sistemas de IA. Paralelamente, avançam as discussões do marco legal da inteligência artificial, representado pelo Projeto de Lei 2338/2023, aprovado pelo Senado e atualmente em análise na Câmara dos Deputados. O projeto propõe uma abordagem baseada em risco, distinguindo sistemas de alto risco, sistemas proibidos e regras específicas para IA generativa, alinhando-se ao movimento internacional por uma regulação clara e humano cêntrica.

Como o gestor pode operacionalizar a governança jurídica da IA nas organizações diante da multiplicidade de normas e frameworks internacionais?

No cenário global, diferentes referências normativas têm orientado organizações sobre como governar e controlar o uso da IA. Uma delas é o NIST AI Risk Management Framework

(AI RMF 1.0), elaborado pelo National Institute of Standards and Technology (EUA), que apresenta quatro funções centrais para a gestão de riscos: Govern, Map, Measure e Manage. Trata-se de um instrumento voluntário, destinado a apoiar o desenvolvimento de sistemas confiáveis e alinhados a valores éticos. Outra base relevante é o ISO/IEC 42001:2023, primeiro padrão internacional de sistema de gestão voltado exclusivamente para IA, que fornece diretrizes para implementação, monitoramento e melhoria contínua de práticas de governança algorítmica dentro de organizações de qualquer porte.

A discussão é especialmente importante para as áreas de administração e direito, pois a IA impacta diretamente temas como responsabilidade civil, governança corporativa, conformidade regulatória (compliance) e controle de riscos. Organizações passam a precisar não apenas de sistemas tecnicamente eficazes, mas também de modelos de gestão capazes de garantir que a tecnologia seja usada de forma ética, segura e conforme a lei. A interdisciplinaridade entre essas áreas torna-se, portanto, indispensável: juristas precisam compreender fundamentos técnicos mínimos, enquanto gestores devem entender obrigações legais, limites regulatórios e princípios de direitos fundamentais.

MARCO CONCEITUAL DA INTELIGÊNCIA ARTIFICIAL E GOVERNANÇA DIGITAL

A crescente incorporação de sistemas de Inteligência Artificial no âmbito das relações sociais, econômicas e institucionais tem provocado transformações significativas na forma como decisões são produzidas, processadas e implementadas. Nesse contexto, o estabelecimento de um marco conceitual acerca da Inteligência Artificial e da Governança Digital constitui elemento fundamental para a compreensão dos impactos jurídicos decorrentes da utilização dessas tecnologias. Conforme destaca Luciano Floridi (2019), a expansão dos sistemas inteligentes exige a reformulação das estruturas tradicionais de responsabilidade, transparência e proteção de direitos, especialmente diante da crescente autonomia decisória dos sistemas algorítmicos. A delimitação conceitual desses temas possibilita não apenas a identificação de seus elementos estruturantes e de suas finalidades, mas também a análise dos desafios relacionados à proteção de direitos fundamentais, à transparência algorítmica, à responsabilidade jurídica, à proteção de dados pessoais e aos mecanismos regulatórios necessários para assegurar o desenvolvimento tecnológico alinhado aos princípios éticos e normativos vigentes. Nesse sentido, Shoshana Zuboff (2019) observa que a consolidação da economia baseada em dados amplia os riscos de assimetria informacional, vigilância e concentração de poder tecnológico, tornando indispensável a criação de mecanismos de governança capazes de limitar abusos e promover accountability. Dessa forma, a compreensão

desses conceitos representa uma etapa essencial para a construção de debates jurídicos consistentes acerca da interação entre inovação tecnológica e ordenamento jurídico contemporâneo.

O QUE É INTELIGÊNCIA ARTIFICIAL NO CONTEXTO ORGANIZACIONAL

A Inteligência Artificial (IA) pode ser entendida como sistemas baseados em máquinas que analisam dados e geram resultados, como previsões, recomendações, conteúdos ou decisões, capazes de influenciar ambientes digitais ou reais. Segundo Organisation for Economic Co-operation and Development (2019), sistemas de IA são capazes de operar com diferentes níveis de autonomia e adaptar seus resultados conforme os objetivos definidos pelos seres humanos. No contexto organizacional, a IA é uma ferramenta estratégica. Empresas e governos utilizam sistemas inteligentes para automatizar tarefas, reduzir custos, melhorar a tomada de decisão e aumentar a eficiência. Nesse sentido, Stuart Russell e Peter Norvig (2021) afirmam que a IA representa um dos principais instrumentos tecnológicos para ampliação da racionalidade computacional aplicada às organizações.

Embora as ferramentas de Inteligência Artificial atuais envolvam técnicas complexas, é possível descrevê-la de forma acessível, separando seu funcionamento em partes, sendo elas:

Algoritmo: conjunto de instruções que diz ao sistema como executar uma tarefa, sendo importante destacar que a área de inteligência artificial engloba diversos algoritmos para a solução de problemas complexos específicos por meio de estratégias que variam desde o processamento de imagens, o processamento de linguagem natural, a classificação, regressão, agrupamento, predição, etc. Para Pedro Domingos (2017), os algoritmos constituem a base do aprendizado computacional moderno, sendo responsáveis pela identificação automatizada de padrões e correlações em grandes volumes de dados.

Amostra de dados: conjunto de dados que representam características de fenômenos do mundo real ou mesmo do mundo digital que servem como base para o processo de treinamento e aprendizado de máquina. Conforme observa Cathy O'Neil (2016), a qualidade e a representatividade dos dados utilizados no treinamento dos sistemas impactam diretamente os resultados produzidos pelos modelos algorítmicos.

Aprendizado de máquina: é o processamento dos dados contidos na amostra de dados por algoritmos de Inteligência Artificial, com o objetivo de identificar padrões, aprendendo a partir de exemplos e melhorando o seu desempenho ao longo do tempo. Segundo Tom Mitchell (1997), um sistema aprende quando consegue aprimorar seu desempenho em determinada tarefa a partir da experiência acumulada.

Modelos generativos: algoritmos de redes neurais, capazes de criar textos, imagens ou outros conteúdos com base em padrões dos dados anteriores. De acordo com Ian Goodfellow et al. (2014), os modelos generativos permitem a produção de conteúdos sintéticos altamente realistas a partir de técnicas avançadas de aprendizado profundo.

Juntos, esses elementos permitem que a IA execute funções antes restritas a seres humanos, como analisar documentos jurídicos, identificar padrões financeiros ou prever comportamentos. Para Kai-Fu Lee (2019), a automação inteligente tende a remodelar profundamente os modelos produtivos e decisórios das organizações contemporâneas.

TIPOS DE INTELIGÊNCIA ARTIFICIAL

IA preditiva: Utiliza dados históricos para estimar o que pode acontecer no futuro. Exemplos comuns incluem previsão de demanda, análise de risco de crédito, identificação de fraudes e manutenção preditiva em operações industriais. Segundo Trevor Hastie, Robert Tibshirani e Jerome Friedman (2009), os modelos preditivos utilizam padrões estatísticos para antecipar comportamentos futuros com base em grandes conjuntos de dados.

IA classificatória: Esse tipo de IA é usada para classificar informações ou pessoas em categorias. Ela é aplicada na triagem de currículos, no reconhecimento de padrões de fraude, na organização de documentos e no apoio a decisões jurídicas. Conforme destaca Virginia Eubanks (2018), sistemas classificatórios automatizados podem influenciar diretamente decisões administrativas e sociais, exigindo mecanismos de supervisão e controle.

IA generativa: Os modelos generativos são capazes de criar conteúdos inéditos: textos, imagens, áudios ou códigos, e vêm ganhando destaque mundial. Segundo OpenAI (2023), os avanços recentes em modelos generativos ampliaram significativamente a capacidade de produção automatizada de conteúdos complexos em linguagem natural.

ONDE A IA É UTILIZADA NAS ORGANIZAÇÕES

A IA está presente em praticamente todas as áreas corporativas e do setor público, conforme exemplos abaixo:

Recursos Humanos (RH): triagem de currículos, previsão de rotatividade, avaliação de desempenho.

Crédito e finanças: análise automática de risco, detecção de anomalias e fraudes.

Marketing: segmentação avançada, personalização de serviços e comportamento do consumidor.

Jurídico: análise de documentos, revisão automatizada de contratos e auxílio em pesquisas jurisprudenciais.

Segurança da informação: detecção de ameaças, identificação de comportamentos suspeitos.

De acordo com Erik Brynjolfsson e Andrew McAfee (2014), a integração da inteligência artificial às organizações representa um dos principais fatores de transformação econômica e produtiva da era digital.

GOVERNANÇA DIGITAL

A Governança Digital refere-se ao conjunto de regras, processos e estruturas que orientam o uso responsável da tecnologia dentro de organizações. Ela garante que a tecnologia seja aplicada de forma ética, segura, transparente e alinhada às metas da instituição. Segundo Luciano Floridi (2018), a governança digital deve estabelecer mecanismos de responsabilização capazes de assegurar que sistemas tecnológicos respeitem direitos fundamentais e valores democráticos.

Organismos internacionais, como a OCDE, reconhecem que a governança de IA é essencial para garantir transparência, responsabilidade e proteção de direitos em ambientes públicos e privados. Os Princípios de IA da OCDE (2019) destacam a necessidade de desenvolvimento de sistemas confiáveis, seguros e centrados no ser humano.

EVOLUÇÃO DO COMPLIANCE DIGITAL

A governança digital é resultado de uma evolução gradual das preocupações jurídicas e tecnológicas e segue as seguintes fases:

1) **Segurança da informação:** triagem de currículos, previsão de rotatividade, avaliação de desempenho. Para Bruce Schneier (2015), a proteção da infraestrutura informacional tornou-se requisito indispensável para a estabilidade das organizações digitais.

2) **Proteção de dados:** Com leis como a LGPD, surgiu a necessidade de orientar o tratamento de dados pessoais com base legal, transparência e garantia de direitos. Segundo Danilo Doneda (2019), a proteção de dados pessoais constitui instrumento essencial para preservação da liberdade e da privacidade na sociedade informacional.

3) **Ética algorítmica:** Com a disseminação da IA, percebeu-se que algoritmos podem gerar efeitos discriminatórios. Organismos como a OCDE criaram princípios de IA voltados para equidade, transparência e respeito aos direitos humanos. Conforme alerta Cathy O'Neil (2016), algoritmos opacos podem reproduzir discriminações estruturais e ampliar desigualdades sociais.

4) **Governança de IA:** Agora, surgem normas específicas para estruturar processos internos de controle, entre as quais temos a ISO/IEC 42001:2023, primeiro padrão internacional de sistema de gestão para IA, que orienta a implementação responsável da tecnologia, e a NIST AI RMF 1.0, modelo que orienta organizações a mapear, medir, gerenciar e mitigar riscos ao longo do ciclo de vida da IA. Temos ainda a regulação brasileira em andamento, como o PL 2338/2023, que propõe regras baseadas em risco para garantir uso ético e seguro da IA. Nesse contexto, National Institute of Standards and Technology (2023) sustenta que a governança da IA deve ser estruturada mediante processos contínuos de avaliação, gerenciamento e mitigação de riscos tecnológicos.

GOVERNANÇA, ACCOUNTABILITY E A MITIGAÇÃO DE RISCOS

A governança só funciona com accountability, isto é, com responsabilidades bem definidas sobre quem desenvolve, implementa, supervisiona e responde pelos impactos da IA. Segundo Mark Bovens (2007), accountability consiste na obrigação de agentes públicos e privados prestarem informações, justificarem suas condutas e se submeterem a mecanismos de controle e responsabilização. Sem isso, organizações ficam vulneráveis a riscos jurídicos, operacionais e reputacionais. Nesse sentido, Luciano Floridi (2018) destaca que a ausência de estruturas claras de responsabilização compromete a confiabilidade e a legitimidade dos sistemas de Inteligência Artificial.

Os princípios internacionais reforçam essa ligação incluem a OCDE, que explica que desenvolvedores e usuários de IA devem ser responsáveis pelo funcionamento dos sistemas e por suas consequências, o NIST AI RMF, que recomenda processos formais e contínuos para identificar, documentar e mitigar riscos, e a ISO/IEC 42001, que exige controles internos, supervisão humana e melhoria contínua para garantir uso responsável e rastreável da IA. De acordo com Organisation for Economic Co-operation and Development (2019), sistemas de IA devem operar de maneira robusta, transparente e passível de supervisão humana ao longo de todo o seu ciclo de vida.

Sendo assim, a governança digital atua como ponte entre tecnologia, gestão e direito, garantindo que sistemas de IA sejam usados de forma segura, ética e conforme a legislação, diminuindo riscos e aumentando a confiança de cidadãos, clientes e reguladores. Para Shoshana Zuboff (2019), mecanismos de governança são indispensáveis para limitar abusos decorrentes da concentração de poder informacional e da exploração massiva de dados.

ART. 20 DA LGPD: DIREITO À REVISÃO DE DECISÕES AUTOMATIZADAS

O art. 20 assegura ao titular o direito de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais e que afetem seus interesses (ex.: crédito, perfil de consumo, bloqueio em plataformas). O controlador deve, quando solicitado, fornecer informações claras sobre os critérios usados, respeitado o segredo comercial; caso não o faça, a ANPD pode auditar para verificar discriminações. Segundo Danilo Doneda (2019), o direito à revisão de decisões automatizadas representa importante mecanismo de proteção da dignidade e da autonomia informacional dos titulares de dados.

Em 2024/2025, a ANPD abriu tomada de subsídios e publicou nota técnica sobre o tema, apontando alguns consensos, a necessidade de transparência e explicabilidade, o uso de salvaguardas técnicas (anonimização e pseudonimização), e avaliações de impacto (RIPD), além de governança e canais para exercer direitos, com debate sobre bases legais e revisão humana. Nesse contexto, Frank Pasquale (2015) sustenta que sistemas algorítmicos opacos podem comprometer direitos fundamentais quando inexistem mecanismos adequados de transparência e supervisão.

A LGPD define controlador (decide sobre o tratamento) e operador (trata em nome do controlador). Ambos podem responder por danos decorrentes de violações. Boas práticas incluem definir papéis, manter registros (art. 37), adotar medidas de segurança e comunicar incidentes quando houver risco relevante. Conforme observa Laura Schertel Mendes (2021), a responsabilização compartilhada entre controlador e operador fortalece a efetividade da proteção de dados pessoais no ambiente digital.

O controlador define finalidades e bases legais, publica informações sobre o tratamento, conduz RIPD quando necessário e responde por danos (art. 42).

O operador executa o tratamento conforme instruções e também pode ser responsabilizado se descumprir a lei ou agir fora das ordens.

Entre as consequências jurídicas de falhas temos as falhas de governança de IA que impliquem violação à LGPD que podem gerar responsabilidade civil por danos materiais e morais, sanções administrativas da ANPD (advertência, multa, publicização) e riscos reputacionais e regulatórios, sendo possível encontrar casos judiciais recentes que ilustram discussões sobre decisões automatizadas e o alcance do art. 20. Para Bruno Bioni (2020), a efetividade da proteção de dados depende da implementação de estruturas concretas de governança e gestão de riscos digitais.

PROJETOS DE LEI E REGULAÇÃO DE IA NO BRASIL

O PL 2.338/2023 (Marco Legal da IA), aprovado no Senado em 10/12/2024 e atualmente em análise na Câmara dos Deputados, propõe uma abordagem baseada em risco, com obrigações proporcionais ao potencial de dano do sistema. Segundo European Commission (2021), modelos regulatórios baseados em risco permitem equilibrar inovação tecnológica e proteção de direitos fundamentais.

Em linhas gerais, o texto e materiais correlatos indicam risco excessivo e inaceitável, incluindo usos proibidos, como a exploração de vulnerabilidades e práticas que violem direitos fundamentais, risco alto, incluindo aplicações críticas como saúde, crédito, educação, segurança pública com obrigações reforçadas (RIPD, governança, supervisão humana, documentação, e riscos limitados e mínimos, como medidas mais leves, focadas em transparência. De acordo com Luciano Floridi et al. (2018), classificações regulatórias por níveis de risco constituem instrumentos relevantes para assegurar proporcionalidade e controle ético sobre sistemas inteligentes.

Esses elementos alinham o Brasil a tendências internacionais de regulação proporcional. Nesse sentido, UNESCO (2021) defende a adoção de estruturas regulatórias capazes de promover inovação responsável, transparência e respeito aos direitos humanos.

O PL reforça deveres de gestão de risco e governança para desenvolvedores e usuários, com ênfase em documentação, monitoramento pós-implantação e prestação de informações. Há propostas de regras de responsabilidade para danos causados por IA (inclusive possibilidade de responsabilidade objetiva em sistemas de alto risco) e mecanismos de fiscalização. Para Cary Coglianese (2021), sistemas regulatórios de IA devem combinar supervisão técnica contínua, transparência organizacional e mecanismos efetivos de accountability.

Situação legislativa (jan/2026): o PL está na Câmara, sob análise em comissão especial, podendo sofrer ajustes antes da votação em plenário.

GUIAS E PADRÕES INTERNACIONAIS QUE ORIENTAM OBRIGAÇÕES

Entre as guias e padrões internacionais temos a OCDE, que rege os princípios do usa da IA e promovem a IA inovadora e confiável, com cinco eixos, a inclusão e bem-estar, os Direitos humanos e valores democráticos, incluindo a privacidade, a transparência, e explicabilidade, a robustez e segurança e a prestação de contas. Segundo a Organisation for Economic Co-operation and Development (2019), sistemas de IA devem ser desenvolvidos de forma centrada no ser humano, respeitando direitos fundamentais, valores democráticos e mecanismos de accountability.

Esses princípios funcionam como base para políticas internas de IA responsável.

Na prática a supervisão humana ocorre de forma proporcional, com testes de viés, documentação e mecanismos de contestação. Para Luciano Floridi et al. (2018), a supervisão humana significativa é indispensável para assegurar controle ético e confiabilidade sobre sistemas automatizados.

Temos também a ecomendação sobre Ética da IA da UNESCO de 2021, que adota uma abordagem global com foco em direitos humanos, dignidade, transparência, equidade e supervisão humana, além de áreas de ação como governança de dados, educação, saúde e meio ambiente. A UNESCO (2021) destaca que a governança ética da IA deve promover inclusão social, diversidade e proteção da dignidade humana. Isso se traduz em práticas internas como códigos de ética, comitês de IA e avaliações de impacto ético.

Temos ainda o Sistema de Gestão de IA ISO/IEC 42001 de 2023, que é o primeiro padrão internacional com requisitos auditáveis para gestão de IA que incluem política, riscos, controles, transparência, supervisão humana e melhoria contínua. Pode ser integrado a outros sistemas ISSO e na prática inclui inventário de sistemas, critérios de risco, métricas e auditorias internas e externas. Segundo a International Organization for Standardization (2023), sistemas de gestão de IA devem operar com processos contínuos de monitoramento, avaliação de riscos e melhoria organizacional.

Por fim temos a Gestão de riscos aplicada à IA NIST AI RMF 1.0, que organiza a gestão de riscos em quatro funções, Govern, Map, Measure, Manage, incluindo diretrizes específicas para IA generativa e orienta o mapeamento de contexto, a análise de riscos, métricas, testes, monitoramento e resposta a incidentes. De acordo com o National Institute of Standards and Technology (2023), a governança de IA exige processos estruturados para identificação, mensuração e mitigação contínua de riscos tecnológicos.

GOVERNANÇA JURÍDICA DA IA NAS ORGANIZAÇÕES

A governança jurídica da Inteligência Artificial é o conjunto de regras, processos e responsabilidades que garantem que sistemas de IA sejam usados de forma ética, segura, transparente e em conformidade com a lei. Ela exige a integração entre áreas como compliance, jurídico, tecnologia da informação, proteção de dados e gestão corporativa, pois nenhum setor isolado consegue lidar sozinho com os riscos e impactos da IA. Segundo Cary Coglianese (2021), a governança algorítmica depende de mecanismos institucionais capazes de integrar supervisão técnica, jurídica e organizacional.

Organismos internacionais, como a OCDE, reforçam que IA responsável depende de transparência, direitos humanos, segurança e accountability, o que exige uma abordagem multidisciplinar dentro das organizações. Para Shoshana Zuboff (2019), a ausência de mecanismos robustos de governança amplia os riscos de concentração de poder informacional e violações de direitos fundamentais.

Padrões como o ISO/IEC 42001 também destacam que a governança de IA deve fazer parte da gestão estratégica, com processos formais, políticas internas e melhoria contínua. A International Organization for Standardization (2023) estabelece que a governança da IA deve estar integrada à estrutura organizacional e às estratégias corporativas.

Para que uma organização consiga aplicar a governança de maneira efetiva, alguns elementos básicos são recomendados por padrões internacionais como ISO/IEC 42001 e pelo NIST AI RMF 1.0, entre os quais temos:

Política de IA responsável: Documento oficial que define princípios, limites, finalidades e critérios éticos para desenvolvimento e uso da IA. Deve seguir valores como transparência, segurança, equidade e supervisão humana, conforme diretrizes da OCDE e UNESCO. Segundo a UNESCO (2021), políticas institucionais de IA devem assegurar respeito à dignidade humana e prevenção de discriminações algorítmicas.

Comitê de Governança de IA: Grupo multidisciplinar com representantes de jurídico, TI, segurança, inovação, RH e compliance. Sua função é avaliar riscos, aprovar projetos, revisar incidentes e acompanhar o ciclo de vida dos sistemas. A ISO 42001 recomenda a inclusão formal dessa estrutura. Conforme aponta Mark Coeckelbergh (2020), estruturas colegiadas e multidisciplinares fortalecem o controle ético sobre decisões automatizadas.

Procedimentos para compras e contratação de tecnologia: Antes de adquirir soluções de IA, a organização deve exigir due diligence técnica e jurídica, verificando riscos, requisitos de segurança, qualidade dos dados e padrões de conformidade. Para Frank Pasquale (2015), mecanismos de avaliação prévia são essenciais para evitar opacidade e assimetria informacional em sistemas automatizados.

Processos formais de aprovação e revisão de sistemas de IA: Inclui análises prévias de impacto, documentação obrigatória e revisão periódica do desempenho, conforme orientações do NIST AI RMF, que prevê funções de mapear, medir e gerenciar riscos. Segundo o National Institute of Standards and Technology (2023), sistemas de IA devem ser submetidos a processos contínuos de validação, monitoramento e gerenciamento de riscos.

Monitoramento contínuo, métricas e indicadores de risco: É essencial acompanhar o funcionamento da IA após a implementação, monitorando viés, erros, segurança,

explainability e robustez, conforme recomendado pelo NIST. De acordo com Cathy O'Neil (2016), sistemas algorítmicos não monitorados tendem a reproduzir vieses e desigualdades em larga escala.

FERRAMENTAS JURÍDICAS ESSENCIAIS PARA A GOVERNANÇA DA IA

A governança da Inteligência Artificial na área jurídica pode ser auxiliada com o uso de ferramentas, como as citadas abaixo:

Auditoria algorítmica: Avaliação periódica para identificar vieses, falhas técnicas, discriminação e falta de transparência. A OCDE reforça a importância da auditabilidade para garantir confiança. Segundo Nicholas Diakopoulos (2016), auditorias algorítmicas são fundamentais para assegurar transparência e controle social sobre sistemas automatizados.

Relatório de Impacto à Proteção de Dados (RIPD): Previsto pela LGPD, o RIPD analisa riscos do tratamento de dados, especialmente em processos automatizados. A ANPD destaca a necessidade de RIPDs para IA e decisões automatizadas. Para Danilo Doneda (2019), relatórios de impacto representam instrumentos preventivos essenciais para redução de danos e fortalecimento da governança de dados.

Matriz de riscos da IA: Ferramenta inspirada nos modelos de risco da ISO 42001 e do NIST, classificando riscos de acordo com impacto, probabilidade, viés, segurança, privacidade e explicabilidade. O National Institute of Standards and Technology (2023) recomenda abordagens estruturadas de classificação e monitoramento de riscos em todo o ciclo de vida da IA.

Gestão de terceiros (due diligence): Avalia fornecedores de IA quanto à conformidade legal, práticas de proteção de dados, segurança e explicabilidade. A ISO 42001 exige controles específicos para relações com terceiros. Segundo Laura Schertel Mendes (2021), a governança de dados exige avaliação contínua de terceiros envolvidos no tratamento automatizado de informações.

Regras internas de explicabilidade e supervisão humana: Atendem a princípios da OCDE e ao NIST, que exigem que sistemas de IA sejam explicáveis, com pontos claros de intervenção humana. Isso reduz riscos e garante accountability. Para Luciano Floridi (2018), a explicabilidade constitui elemento indispensável para legitimar decisões automatizadas em ambientes democráticos.

Vale ressaltar que a governança jurídica da IA exige modelo multidisciplinar, estruturas bem definidas e ferramentas de controle que combinem aspectos técnicos, jurídicos e organizacionais. Padrões confiáveis, como OCDE, UNESCO, ISO/IEC 42001 e NIST AI

RMF que dão suporte para que empresas e instituições públicas adotem práticas seguras, éticas e alinhadas ao direito. Segundo Cary Coglianese (2021), a governança algorítmica eficiente depende da integração entre regulação, gestão de riscos e supervisão institucional contínua.

O PAPEL DO GESTOR COMO AGENTE DE CONFORMIDADE DIGITAL

No contexto da Inteligência Artificial (IA), o gestor assume um papel central, ele atua como ponte entre o jurídico, a tecnologia e a direção estratégica da organização. Esse papel é reforçado por padrões internacionais, como os Princípios de IA da OCDE, que destacam a importância de transparência, responsabilidade e supervisão humana. Para Peter Drucker (1999), a gestão moderna exige capacidade de adaptação estratégica diante das transformações tecnológicas e informacionais.

Da mesma forma, o ISO/IEC 42001:2023 exige que a alta gestão assuma responsabilidade direta pela governança de IA, integrando aspectos técnicos, jurídicos e organizacionais. A International Organization for Standardization (2023) reforça que a liderança organizacional deve assumir compromisso ativo com a implementação responsável da IA.

Assim, o gestor precisa compreender simultaneamente, analisar riscos operacionais, como falhas técnicas, baixa qualidade de dados, vieses e problemas de segurança, riscos jurídicos, como violações à LGPD, decisões automatizadas sem supervisão, descumprimento de padrões internacionais e impactos éticos e reputacionais, como discriminação algorítmica, falta de transparência e danos à confiança. Segundo Cathy O'Neil (2016), decisões automatizadas sem monitoramento adequado podem reproduzir discriminações sistêmicas e gerar impactos sociais relevantes.

Para exercer esse papel com segurança e responsabilidade, o gestor precisa desenvolver competências essenciais como Alfabetização em IA suficiente para compreender como modelos funcionam, seus limites e riscos, requisito alinhado aos princípios de explicabilidade da OCDE, a capacidade de interpretar relatórios técnicos, o entendimento dos requisitos da LGPD, especialmente os relacionados a decisões automatizadas (art. 20), transparência e necessidade, a liderança em ambientes tecnológicos, com destaque em saber coordenar equipes multidisciplinares (jurídico, TI, segurança e dados), conforme exigido pelo sistema de gestão da ISO 42001, e a capacidade de tomada de decisão baseada em dados. De acordo com Erik Brynjolfsson e Andrew McAfee (2014), a capacidade analítica orientada por dados tornou-se competência central das lideranças organizacionais contemporâneas.

O gestor possui ainda responsabilidades práticas e deve transformar princípios e exigências legais em ações concretas dentro da organização, definindo políticas internas e fluxo

de aprovação, criar documentos oficiais que regulem o desenvolvimento e uso de IA, conforme recomendações da ISO 42001 e critérios éticos da UNESCO, garantindo a supervisão humana significativa, obrigação prevista na LGPD e reforçada pela OCDE como requisito para IA confiável, estabelecendo canais para contestação de decisões automatizadas, garantindo ao titular o direito de solicitar revisão humanizada, exigindo que o gestor crie canais eficientes, realizando treinamentos obrigatórios para que toda a equipe conheça riscos, tenha boas práticas e saiba dos requisitos legais, medida promovida pela OCDE e UNESCO como base da governança ética, assegurando assim a conformidade com legislações e padrões internacionais

O gestor deve acompanhar LGPD, PL 2.338/2023, OCDE, UNESCO, ISO 42001 e NIST para manter a organização atualizada e segura. Segundo Cary Coglianese (2021), a conformidade digital exige monitoramento regulatório contínuo e adaptação permanente às mudanças tecnológicas.

As consequências de uma má gestão incluem riscos jurídicos que podem envolver multas, sanções da ANPD e processos judiciais por falhas, discriminação algorítmica ou vazamentos, riscos reputacionais, que podem envolver perda de confiança de consumidores e parceiros, amplamente destacada em diretrizes éticas internacionais e riscos técnicos, que incluem falhas de sistemas, ataques cibernéticos, vieses e uso inadequado de dados, alertados pelo NIST e pela OCDE. Para Shoshana Zuboff (2019), a perda de confiança digital constitui um dos principais impactos negativos decorrentes do uso irresponsável de tecnologias baseadas em dados.

ESTUDOS DE CASO

Caso 1 - Viés em triagem de currículos: Amazon Recruiting Bias AI

O sistema de inteligência artificial desenvolvido pela Amazon para automatizar a seleção de currículos. Treinado com dados históricos predominantemente masculinos, o algoritmo passou a favorecer homens e a penalizar candidatas mulheres, reproduzindo vieses discriminatórios existentes nos dados utilizados. O episódio tornou-se um dos principais exemplos dos riscos da IA em processos decisórios, evidenciando problemas relacionados à discriminação algorítmica, falta de transparência e necessidade de governança, supervisão humana e regulação no uso da inteligência artificial.

Caso 2 - Análise de Crédito: Apple Card

Este tornou-se um dos exemplos mais conhecidos de riscos da inteligência artificial em análise de crédito. Clientes relataram que o sistema automatizado concedia limites significativamente menores para mulheres, mesmo quando possuíam renda e histórico financeiro semelhantes aos de homens. Desenvolvido pela Apple em parceria com o Goldman Sachs, o modelo foi criticado pela falta de transparência e pela dificuldade de explicar os critérios utilizados nas decisões. O episódio evidenciou problemas de opacidade algorítmica e possível discriminação automatizada, reforçando a necessidade de auditoria, explicabilidade, supervisão humana e governança de IA para reduzir riscos jurídicos e garantir maior confiança dos consumidores.

Caso 3 - Setor Público: Caso Robert Williams

Ocorrido em Detroit, tornou-se um dos exemplos mais conhecidos dos riscos da inteligência artificial no setor público. Robert Williams foi preso injustamente após um sistema de reconhecimento facial utilizado pela polícia identificá-lo erroneamente como suspeito. O episódio evidenciou falhas da IA, especialmente vieses raciais e falta de transparência, reforçando a necessidade de supervisão humana, auditoria e governança ética no uso de tecnologias pelo poder público.

PROPOSTA DE UM FRAMEWORK DE GOVERNANÇA DE IA

A proposta é reunir os passos essenciais de um modelo, ou um “esqueleto” pré-definid, de governança de IA, alinhado às melhores práticas internacionais, como o ISO/IEC 42001, que exige gestão estruturada e rastreabilidade das decisões; o NIST AI RMF, que orienta a identificação e mitigação de riscos; e os princípios de transparência e responsabilidade da OCDE. Segundo Cary Coglianese (2021), frameworks de governança algorítmica são fundamentais para estruturar mecanismos de supervisão, controle e responsabilização no uso da Inteligência Artificial.

O framework propõe os seguintes passos:

1) Inventário dos sistemas de IA

Registrar todos os sistemas que usam IA, internos ou de fornecedores, com informações sobre: finalidade, dados utilizados, responsáveis e área usuária. O ISO 42001 exige

esse mapeamento para garantir rastreabilidade e controle. A International Organization for Standardization (2023) destaca que o inventário de sistemas é requisito essencial para assegurar governança, transparência e monitoramento contínuo da IA.

2) Classificação de risco

Avaliar cada sistema e classificá-lo como baixo, médio ou alto risco, considerando o impacto sobre pessoas, possibilidade de vieses, o uso de dados pessoais, as dependências de decisões automatizadas. Segundo a European Commission (2021), abordagens regulatórias baseadas em risco permitem aplicar medidas proporcionais conforme o potencial de impacto dos sistemas de IA.

3) Avaliação jurídica e técnica

Antes de aplicar ou expandir sistemas de IA, devem ser avaliados a base legal (LGPD, a necessidade de RIPD ou documentação do risco (art. 20 para decisões automatizadas), os riscos técnicos, como segurança, robustez e vieses. A LGPD exige revisão humana e transparência em decisões automatizadas. Para Danilo Doneda (2019), avaliações prévias de impacto são indispensáveis para assegurar proteção de direitos fundamentais e prevenção de danos no tratamento automatizado de dados.

4) Definição de supervisão humana

Determinar quando a intervenção humana será obrigatória e quem será o responsável por revisões críticas. A OCDE destaca supervisão humana como elemento essencial para evitar danos. A UNESCO reforça a centralidade humana e a necessidade de escolhas informadas. Segundo Luciano Floridi et al. (2018), a supervisão humana significativa constitui requisito indispensável para garantir legitimidade ética e jurídica aos sistemas automatizados.

5) Controles e métricas

Estabelecer indicadores para monitorar o sistema, como a precisão, a taxa de erro, os indicadores de viés, a segurança da informação e a explicabilidade. Tanto o NIST quanto o ISO 42001 recomendam métricas contínuas para manter confiabilidade. De acordo com o National Institute of Standards and Technology (2023), métricas contínuas de monitoramento são essenciais para avaliar desempenho, robustez e riscos de sistemas de IA.

6) Auditoria contínua

Realizar auditorias periódicas para detectar falhas, vieses, erros e riscos emergentes. O ISO 42001 inclui auditorias internas e monitoramento sistemático de riscos. Para Nicholas Diakopoulos (2016), auditorias algorítmicas fortalecem a transparência e a responsabilização institucional sobre decisões automatizadas.

7) Relatórios de transparência

Gerar documentos claros que expliquem a finalidade do sistema, os critérios usados para decisões, os riscos identificados e os canais para contestação. A OCDE e a LGPD exigem transparência e direito à explicação. Segundo Frank Pasquale (2015), a transparência algorítmica constitui mecanismo essencial para limitar opacidade e assimetrias de poder na sociedade digital.

8) Revisão periódica

Atualizar modelos, políticas internas, contratos e controles de acordo com mudanças técnicas, regulatórias e organizacionais. A ISO 42001 orienta revisão contínua dentro do ciclo de melhoria (PDCA). A International Organization for Standardization (2023) estabelece que sistemas de gestão de IA devem operar sob melhoria contínua e adaptação permanente aos riscos emergentes.

O framework propõe mapear, classificar riscos, avaliar legal e tecnicamente, garantir supervisão humana, monitorar métricas, auditar, ser transparente e revisar continuamente o uso da IA, tudo alinhado às exigências da LGPD e às melhores práticas internacionais. Segundo Cary Coglianese (2021), modelos estruturados de governança permitem equilibrar inovação tecnológica, gestão de riscos e proteção de direitos fundamentais.

CONCLUSÃO

A transformação digital impulsionada pela Inteligência Artificial exige que as organizações adotem governança jurídica sólida e estruturada. Diante dos riscos técnicos, éticos e jurídicos envolvidos, fica evidente que a governança não é opcional, mas um requisito essencial para proteger direitos, reduzir incertezas e garantir conformidade com marcos normativos como a LGPD, além de padrões internacionais de governança e risco. Para Shoshana Zuboff (2019), a ausência de governança adequada pode ampliar vulnerabilidades sociais, econômicas e informacionais em larga escala.

O gestor desempenha um papel central nesse cenário. Ele atua como o elo entre tecnologia, jurídico e estratégia, garantindo que decisões automatizadas sejam transparentes,

auditáveis e alinhadas a princípios de ética e responsabilidade. Sem essa atuação integrada, cresce o risco de vieses, violações legais e danos reputacionais. Segundo Peter Drucker (1999), a gestão eficiente depende da capacidade de integrar inovação, responsabilidade e tomada de decisão estratégica.

Nesse contexto, o gestor pode operacionalizar a governança jurídica da Inteligência Artificial por meio da criação de políticas internas de uso da IA, mecanismos de controle de riscos e procedimentos de supervisão humana. Para isso, deve integrar requisitos jurídicos, éticos e técnicos às atividades da organização, garantindo transparência, segurança, proteção de dados e responsabilização nas decisões automatizadas. De acordo com Luciano Floridi (2018), a governança ética da IA exige integração entre tecnologia, responsabilidade institucional e proteção dos direitos humanos.

A aplicação prática dessa governança ocorre com a adoção de frameworks internacionais, como os princípios da Organisation for Economic Co-operation and Development (OCDE), o AI Risk Management Framework do National Institute of Standards and Technology (NIST) e a norma ISO/IEC 42001, que orientam a gestão de riscos, auditoria, transparência e conformidade regulatória. Além disso, o gestor deve promover treinamento das equipes, avaliações de impacto algorítmico e monitoramento contínuo dos sistemas de IA, assegurando compatibilidade com direitos fundamentais e com a legislação vigente, especialmente em matéria de proteção de dados e não discriminação. Segundo a UNESCO (2021), a governança ética da IA depende da combinação entre capacitação institucional, transparência e supervisão contínua.

A experiência internacional demonstra que a IA só é sustentável quando operada com transparência, ética e supervisão humana, elementos reforçados por organismos como a OCDE, UNESCO e pelos frameworks NIST e ISO/IEC 42001. Esses princípios asseguram que a tecnologia gere valor sem comprometer direitos fundamentais. Para Mark Coeckelbergh (2020), a sustentabilidade da IA depende da construção de confiança social baseada em responsabilidade, transparência e controle humano.

Por fim, organizações que se adaptam rapidamente, adotando políticas claras, controles robustos e práticas responsáveis, obtêm vantagem competitiva. Elas inspiram confiança, reduzem riscos e conseguem utilizar a IA de forma estratégica, segura e alinhada aos valores jurídicos e sociais que orientam a sociedade. Segundo Erik Brynjolfsson e Andrew McAfee (2014), organizações capazes de integrar inovação tecnológica e governança eficiente tendem a alcançar maior competitividade e sustentabilidade no ambiente digital.

REFERÊNCIAS BIBLIOGRÁFICAS

ANPD. *Documentos técnicos e orientativos*. Brasília, DF, 2025. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-tecnicos-e-orientativos. Acesso em: 12 jan. 2026.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. 2. ed. Rio de Janeiro: Forense, 2020.

BOVENS, Mark. Analysing and assessing accountability: a conceptual framework. *European Law Journal*, v. 13, n. 4, p. 447–468, 2007.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*. Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 abr. 2026.

BRASIL. Projeto de Lei nº 2.338/2023. Texto consolidado aprovado em comissão. Brasília, DF, 2025. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 17 maio 2026.

BRASIL. Senado Federal. *Lei Geral de Proteção de Dados Pessoais: edição atualizada até junho de 2024*. Brasília, DF: Senado Federal, 2024. Disponível em: https://www2.senado.leg.br/bdsf/handle/id/665448. Acesso em: 2 maio 2026.

BRASIL. Senado Federal. Projeto de Lei nº 2.338, de 2023. Dispõe sobre o uso da inteligência artificial no Brasil. Brasília, DF: Senado Federal, 2023. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em: 26 mar. 2026.

BRYNJOLFSSON, Erik; MCAFEE, Andrew. *The second machine age: work, progress, and prosperity in a time of brilliant technologies*. New York: W. W. Norton & Company, 2014.

COECKELBERGH, Mark. *AI ethics*. Cambridge: MIT Press, 2020.

COGLIANESE, Cary. *Algorithmic accountability and governance*. Philadelphia: University of Pennsylvania Law School, 2021.

CONVERGÊNCIA DIGITAL. ANPD dá prioridade à regulação de decisões automatizadas por IA. São Paulo, 20 maio 2025. Disponível em: https://convergenciadigital.com.br. Acesso em: 7 maio 2026.

DIAKOPOULOS, Nicholas. Accountability in algorithmic decision making. *Communications of the ACM*, v. 59, n. 2, p. 56–62, 2016.

DOMINGOS, Pedro. *O algoritmo mestre*. São Paulo: Novatec, 2017.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

DRUCKER, Peter. *Desafios gerenciais para o século XXI*. São Paulo: Pioneira, 1999.

EUBANKS, Virginia. *Automating inequality: how high-tech tools profile, police, and punish the poor*. New York: St. Martin's Press, 2018.

EUROPEAN COMMISSION. *Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Brussels, 2021.

FLORIDI, Luciano. Establishing the rules for building trustworthy AI. *Nature Machine Intelligence*, v. 1, p. 261–262, 2019.

FLORIDI, Luciano. Soft ethics and the governance of the digital. *Philosophy & Technology*, v. 31, p. 1–8, 2018.

FLORIDI, Luciano et al. AI4People—an ethical framework for a good AI society. *Minds and Machines*, v. 28, p. 689–707, 2018.

GOODFELLOW, Ian et al. Generative adversarial nets. In: *Advances in Neural Information Processing Systems*. [S. l.]: NeurIPS, 2014.

HASTIE, Trevor; TIBSHIRANI, Robert; FRIEDMAN, Jerome. *The elements of statistical learning*. 2. ed. New York: Springer, 2009.

IEC. *ISO/IEC 42001:2023 – Artificial intelligence — Management system*. Geneva: International Electrotechnical Commission, 2023. Disponível em: https://webstore.iec.ch. Acesso em: 19 set. 2025.

ITS RIO. *100 IA: PL 2.338/2023 e a classificação de risco dos usos de IA sob uma perspectiva prática*. Rio de Janeiro, 2024. Disponível em: https://itsrio.org. Acesso em: 11 fev. 2026.

ISO. *ISO/IEC 42001:2023 – Artificial intelligence — Management system*. Geneva: International Organization for Standardization, 2023. Disponível em: https://www.iso.org. Acesso em: 27 nov. 2025.

JUSBRASIL. Artigo 20 da Lei nº 13.709, de 14 de agosto de 2018. São Paulo, 2024. Disponível em: https://www.jusbrasil.com.br. Acesso em: 9 maio 2026.

LEE, Kai-Fu. *AI superpowers: China, Silicon Valley, and the new world order*. Boston: Houghton Mifflin Harcourt, 2019.

LIBRARY OF CONGRESS. Brazil: Senate advances discussions on bill to regulate AI use. Washington, D.C., 23 maio 2025. Disponível em: https://www.loc.gov. Acesso em: 8 maio 2026.

MARANHÃO, Juliano; VAINZOF, Rony; FICO, Bernardo. Riscos e oportunidades da regulamentação de decisões automatizadas e inteligência artificial pela ANPD. *Consultor Jurídico*, 27 nov. 2024. Disponível em: https://www.conjur.com.br. Acesso em: 6 maio 2026.

MELCHIOR, Camila; FERNANDES, Micaela. O artigo 20 da LGPD e os desafios interpretativos. 2020. Disponível em: https://www.academia.edu. Acesso em: 17 jan. 2026.

MENDES, Laura Schertel. *Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação*. São Paulo: Thomson Reuters Brasil, 2021.

MITCHELL, Tom. *Machine learning*. New York: McGraw-Hill, 1997.

NIST. *AI Risk Management Framework*. Gaithersburg, 2024. Disponível em: https://www.nist.gov/itl/ai-risk-management-framework. Acesso em: 8 maio 2026.

NIST. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg: National Institute of Standards and Technology, 2023. Disponível em: https://nvlpubs.nist.gov. Acesso em: 29 out. 2025.

NIST. *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (AI 600-1)*. Gaithersburg, 2024. Disponível em: https://www.nist.gov. Acesso em: 26 abr. 2026.

O'NEIL, Cathy. *Weapons of math destruction*. New York: Crown Publishing Group, 2016.

OECD. *Artificial Intelligence Principles*. Paris: OECD, 2019. Atualizado em 2024. Disponível em: https://oecd.ai/en/ai-principles. Acesso em: 17 maio 2026.

OECD. *Governing with artificial intelligence: are governments ready?* Paris: OECD, 2024. Disponível em: https://www.oecd.org. Acesso em: 22 abr. 2026.

OECD. *OECD principles on artificial intelligence*. Paris: OECD Publishing, 2019.

OECD.AI. *AI Principles*. Paris, 2024. Disponível em: https://oecd.ai. Acesso em: 3 mar. 2026.

OECD.AI. *AI Principles Overview*. Paris, 2024. Disponível em: https://oecd.ai/en/ai-principles. Acesso em: 17 maio 2026.

OPENAI. *GPT-4 technical report*. 2023. Disponível em: https://arxiv.org/abs/2303.08774. Acesso em: 17 maio 2026.

PASQUALE, Frank. *The black box society: the secret algorithms that control money and information*. Cambridge: Harvard University Press, 2015.

PIRONTI, Rodrigo. Afinal, quem é considerado operador de dados na LGPD. *Consultor Jurídico*, 26 abr. 2022. Disponível em: https://www.conjur.com.br. Acesso em: 21 mar. 2026.

RUSSELL, Stuart; NORVIG, Peter. *Artificial intelligence: a modern approach*. 4. ed. Pearson, 2021.

SCHNEIER, Bruce. *Data and Goliath: the hidden battles to collect your data and control your world*. New York: W. W. Norton & Company, 2015.

SINDPD. Regulamentação da IA priorizará decisões automatizadas. São Paulo, 21 maio 2025. Disponível em: https://sindpd.org.br. Acesso em: 3 maio 2026.

UNESCO. *Recommendation on the ethics of artificial intelligence*. Paris: UNESCO, 2021. Disponível em: https://unesdoc.unesco.org. Acesso em: 21 dez. 2025.

ZUBOFF, Shoshana. *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs, 2019.